IDA

INSTITUTE FOR DEFENSE ANALYSES

National Comparative Risk Assessment Pilot Project

Cyber Intrusion Analysis–Process Control System

William R. Simpson, Task Leader
Reginald N. Meeson

June 2007

IDA Paper P-4226
Log: H 07-000572

This work was conducted under contract DASW01-04-C-0003, Task ER-6-2474, for the Department of Homeland Security. The publication of this IDA document does not indicate endorsement by the Department of Defense, nor should the contents be construed as reflecting the official position of the Agency.

INSTITUTE FOR DEFENSE ANALYSES

IDA Paper P-4226

National Comparative Risk Assessment Pilot Project

Cyber Intrusion Analysis–Process Control System

William R. Simpson, Task Leader
Reginald N. Meeson

Preface

This document was prepared by the Institute for Defense Analyses (IDA) under the task order Expanded National Comparative Risk Assessment Model (NCRA-2) for the Department of Homeland Security for the Risk Management Division. It partially fulfills the objectives of the task to develop a Common Risk Methodology for critical infrastructure elements.

The Delphi Group was formed to provide an evaluation of cyber threats, possible defensive configurations and the efficacy of those configurations in defending process control systems against those cyber threats. The authors would like to thank the following who, together with the authors formed the Delphi Group: Dr. Gregory N. Larsen, Dr. Edward A. Schneider and Mr. David A. Wheeler.

This document was reviewed by IDA research staff members, Ms. Priscilla Guthrie, Dr. Gregory N. Larsen, Mr. James D. Morgeson, Dr. Edward A. Schneider, Dr. Alan H. Shaw and Mr. David A. Wheeler.

Contents

PREFACE iii

CONTENTS v

FIGURES ix

TABLES xi

EXECUTIVE SUMMARY ES-1

1. BACKGROUND 1

1.1 HOMELAND SECURITY ACT OF 2003 (PD-7) 1
1.2 INITIAL PILOT PROJECT (IDA D-3309) 1
1.3 GOALS OF THIS ANALYSIS 2
1.4 SCOPE LIMITATION 2
1.4.1 Oil and Gas 3
1.4.2 Electric Power Production 3

2. THE ENVIRONMENT 5

2.1 CYBER DEFENSES 5
2.2 CYBER SECURITY 6
2.3 THE PROCESS CONTROL SYSTEM 7
2.3.1 Growth in use of IT 8
2.3.2 Move toward standard interfaces 8
2.3.3 Market and competition pressures among critical infrastructure elements 9
2.4 IT TRENDS 9

3. ASSESSMENT MODELING APPROACH 11

3.1 MODELING APPROACH AND RESULTS OF IDA D-3309 11
3.2 DATA GATHERING THROUGH INDUSTRY WORKING GROUPS 12
3.2.1 Oil and Gas 12
3.2.2 Electric Power Production 12
3.3 MODIFIED DELPHI APPROACH AND PARTICIPANTS 13
3.4 VALIDATION PROCESS 13

4. CYBER DEFENSIVE CONFIGURATIONS 15

4.1 THE PCS (FUNCTIONALLY) 15
4.2 CORPORATE/MARKETING/PCS COMMON ELEMENTS 16
4.3 BASIC TYPES OF LAN/WAN IN THE PCS 16
4.3.1 Integrated 17
4.3.2 Separated 17
4.3.3 Isolated 18
4.4 APPROACH TO ENUMERATION OF CDCS FOR PCS SYSTEMS 19
4.5 APPLYING THE BUILDING BLOCKS 20
4.6 THE CDCS FOR PCS SYSTEMS 21
4.6.1 Cyber Defensive Configuration 1 - Integrated 22
4.6.2 Cyber Defensive Configuration 2 – Integrated 23
4.6.3 Cyber Defensive Configuration 3 – Integrated 24
4.6.4 Cyber Defensive Configuration 4 – Integrated 25

4.6.5 Cyber Defensive Configuration 5 – Integrated 26
4.6.6 Cyber Defensive Configuration 6 – Integrated 26
4.6.7 Cyber Defensive Configuration 7 – Separated 26
4.6.8 Cyber Defensive Configuration 8 – Separated 27
4.6.9 Cyber Defensive Configuration 9 – Separated 28
4.6.10 Cyber Defensive Configuration 10 – Separated 28
4.6.11 Cyber Defensive Configuration 11 – Separated 28
4.6.12 Cyber Defensive Configuration 12 – Isolated 29
4.6.13 Cyber Defensive Configuration 13 – Isolated 30
4.6.14 Cyber Defensive Configuration 14 – Isolated 31
4.6.15 Cyber Defensive Configuration 15 – Isolated 31
4.7 CDCs for Corporate LAN 31
4.8 Survey questions for establishing defensive configurations for PCS Systems 32

5. THREAT SCENARIOS 35

5.1 General 35
5.1.1 Cyber Attack vectors for the enumerated CDCs 35
5.2 Threat1 – T1 35
5.3 Threat2 – T2 36
5.4 Threat3 – T3 36

6. ENUMERATED PROBABILITIES OF SUCCESS WITH AN ATTACK GIVEN 37

6.1 Delphi Deliberations 37
6.2 Refinements to the Figures 38
6.3 Probabilities of Success Approximated for Corporate LANS 41
6.4 Consideration of Best Practices 41
6.5 Computation of Probability of Success Given an Attack 42

7. MATCHING SURVEY RESPONSES TO THE CDCS AND OBTAINING AN ANALYSIS VALUE OF PROBABILITY OF SUCCESS 43

7.1 Survey Responses 43
7.2 Computation 43
7.3 Example Computations 43
7.3.1 An Example with a Match to a CDC 43
7.3.2 An Example without a Match to a CDC 44

8. CONSEQUENCE CALCULATION 45

8.1 Consequence Issues 45
8.2 Data Sources 45
8.3 Threat 1 – Electrical Power Disruption 47
8.4 Threat 1 – Gas Pipeline Disruption 47
8.5 Threat 2 – Electrical Power Disruption 48
8.6 Threat 2 – Gas Pipeline Disruption 48
8.7 Threat 3 – Electrical Power Disruption 48
8.8 Threat 3 – Oil Platform Disruption 49

9. CONDITIONAL RISK CALCULATIONS 51

9.1 Spot Terrorist Threat 1 51
9.2 Criminal Extortion Threat 2 52
9.3 Coordinated Terrorist Threat 3 54

10. CONCLUSIONS 58

10.1 The following conclusions are derived from this analysis 58

11. RECOMMENDATIONS **60**

11.1 THE FOLLOWING RECOMMENDATIONS ARE MADE: **60**

APPENDIX A DEFINITIONS AND ACRONYMS **A-1**

APPENDIX B REFERENCES **B-1**

APPENDIX C DELPHI PARTICIPANTS AND RELEVANT EXPERIENCE **C-1**

APPENDIX D QUESTIONNAIRE DATA RELEVANCE **D-1**

APPENDIX E VALIDATION REVIEW DATA **E-1**

WORKING DEFINITIONS **E-1**

SUMMARIES OF VALIDATION MEETING PARTICIPANTS **E-1**

Chris Barrett, Ph.D. **E-1**

Newton Howard, Ph.D. **E-2**

Michael B. Lombard **E-2**

Figures

Figure 1. Process Control System 15

Figure 2. Basic Elements of the Corporate Network When PCS Elements are Present 16

Figure 3. Integrated PCS 17

Figure 4. Separated PCS 18

Figure 5. Isolated PCS 18

Figure 6. Defensive Configuration Buildup 19

Figure 7. CDC Buildup 21

Figure 8. Cyber Defense Configuration 1 23

Figure 9. Cyber Defense Configuration 2 24

Figure 10. Cyber Defense Configuration 3 25

Figure 11. Cyber Defense Configuration 7 27

Figure 12. Cyber Defense Configuration 12 30

Figure 13. Successful Defense 38

Figure 14. Cross Plot Smoothing 41

Figure 15. Notional Production Loss from Spot Terrorist Attack 47

Figure 16. Notional Production Losses for Large-Scale Terrorist Attack 49

Figure 17. Conditional Risk for the Spot Terrorist Threat 52

Figure 18. Conditional Risk for Cyber Extortion 54

Figure 19. Conditional Risks for the Large-Scale Terrorist Threat 55

Tables

Table 1. Defensive Configurations 22

Table 2. Corporate LAN Configurations 32

Table 3. Probability of Success Given an Attack for CDC and Threat 37

Table 4. Relative Ranking of Defenses 39

Table 5. Relative Ratios 40

Table 6. Probability of Success Given an Attack for Corporate LAN Configurations 41

Table 7. Penalty for Violation of Best practice 42

Table 8. Recovery schedule for a major electrical power outage 49

Table 9. Conditional Risk for the Spot Terrorist 51

Table 10. Conditional Risk for the Criminal Extortion 53

Table 11. Conditional Risk for the Large-Scale Terrorist Threat 55

Table D-1. Survey Questions Answered for Each of the CDCs D-1

Table D-2. CDC Uniqueness Test D-1

Executive Summary

The Homeland Security Act of 2003 and the Homeland Security Presidential Directive 7 call for the Department of Homeland Security to conduct comprehensive assessments of the nation's critical infrastructure as well as establish uniform policies, approaches, guidelines and methodology for integrating Federal infrastructure and protection and *risk management* activities. An initial pilot project was undertaken to define a common risk model with common methodologies and approved scales to measure key parameters to accelerate the progress toward the stated goals of the Department in risk assessment activities. This report describes an extension of that analysis to the area of risk assessment for cyber attacks. This involves defining cyber threats, the basic building blocks of security systems, and Cyber Defensive Configurations (CDCs) that are made up of building blocks and are reasonable representations of actual systems, the development of scenarios for consequence evaluation, and notional examples of the computations. These steps were validated by a team of independent subject matter experts, entirely separate from the IDA team that conducted the research.

The analysis found that:

1. Objectively identifying CDC are possible through the use of simple questionnaires. (Answering the questions may not be so simple).

2. The definition of an asset must be developed by elements of the infrastructure and the asset owner.

3. Actual accident/incident data provides an excellent start for consequence data.

4. Consequence data are best developed by asset owners.

5. The Common Risk Model can be applied to cyber intrusion scenarios.

6. The Common Risk Model should only be used for relative ranking of cyber conditional risks and the absolute values computed may contain inaccuracies.

7. Probabilities of success given an attack, while subjective, represent reasonable relative positions of cyber defense effectiveness.

The report recommends that:

1. Threat attributes and potential threats for these analyses should be separated and deliberately crafted.

2. The analysis should be extended to the general case of IT infrastructure as part of a critical infrastructure operation. This analysis was limited to the process control system aspects.

3. The analysis process should be made available to asset owners in the critical infrastructure with training as needed.

4. This analysis process for cyber security should be refined by successive iteration and input from asset owners.

5. Specific asset owners should be selected to create working examples for the purpose of developing Return On Investment (ROI) models for security measures.

1. Background

1.1 Homeland Security Act of 2003 (PD-7)

The Homeland Security Act of 2003 and the Homeland Security Presidential Directive 7 call for the Department of Homeland Security to conduct comprehensive assessments of the nation's critical infrastructure as well as establish uniform policies, approaches, guidelines and methodology for integrating Federal infrastructure and protection and *risk management* activities. In response to these, Secretary Chertoff, in the Preface to the 2006 National Infrastructure Protection Plan (NIPP)[1], states that the plan "sets forth a comprehensive risk management framework…" The remainder of the document stops short of specifying a common risk model and the uniform methods and scales necessary to implement such a framework.

1.2 Initial Pilot Project (IDA Document D-3309)

An initial pilot project was undertaken to define such a common risk model with common methodologies and approved scales to measure key parameters to accelerate the progress toward the stated goals of the Department in risk assessment activities. The results of this modeling activity were presented in IDA Document D-3309[2]. The report discussed the common risk model and gave examples of its use in the kinetic attack scenario by terrorist threats.

The initial applications of the model concentrated on terrorist attacks using kinetic explosives over a range of infrastructure elements with various forms of defenses in place. A finite number of defensive configurations were mapped and using satellite imagery and other intelligence, defensive configurations for various elements of the infrastructure were determined. Probabilities of success were assigned by subject matter experts and examples were produced that provided a model that effectively supports the decision needs for comparative risk assessment, is credible and understandable, consistent and objective, mathematically defensible, and extensible. The model is discussed in detail in Chapter 3.

---

[1] U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, Washington DC, 2006.

[2] J. D. Morgeson, et al., Institute for Defense Analyses, *National Comparative Risk Assessment Pilot Project*, IDA Document D-3309, 2006.

1.3 Analysis Goals

The goal of this analysis is to extend the referenced applications to the area of cyber attacks. This involves the developing cyber threats, the basic building blocks of security systems, and Cyber Defensive Configurations (CDCs) that are made up of the building blocks and are reasonable representations of actual systems. Also, the gathering of subject matter experts to review these CDCs and to place a worth value or defensive capability of these CDCs, and to put together scenarios for consequence evaluation. Because of the granularity of the analysis, the strength of mechanism of security products will not be designated. It is assumed, however, that as the overall security posture is elevated that weaker elements will be replaced by stronger or strengthened elements (i.e., locks being re-keyed or replaced with stronger locks in the example in chapter 2).

1.4 Scope Limitation

The critical infrastructure IT systems of interest were the process control systems (PCS) and the PCS were considered the target of the postulated threats. PCS systems are used in a wide variety of critical infrastructure elements, including chemical plants, electric production and oil and gas production among others. These analyses are applicable to chemical, energy, nuclear facilities, telecoms, water treatment and food processing. These analyses probably do not apply to banking and financial organizations. Aspects of these analyses may apply to commercial assets, defense industrial base, national monuments and icons, postal and shipping, and transportation where process control systems are present.

The definition of an asset needs to be expanded beyond the referenced study, D-3309, because PCS systems may contain a combination of assets used in the process. For example, electric power production may include many plants and transmission facilities to effectively produce electric power for the national grid system. The asset for cyber events is the collection of facilities and processes that together form the process control system. The definition of these assets and their inter-relations are best developed by the asset owners. Unlike physical configurations, satellite data are not of much value in figuring the installed cyber defensive capabilities of IT systems. While a set of defensive configurations have been developed, any particular infrastructure asset owner will have to evaluate which defensive configuration best represents his IT infrastructure. It is realized that defensive configurations in the cyber area are a spectrum and therefore approaches to interpolating between defensive configurations were developed. Finally, consequence data were taken from two representative infrastructure elements; oil and gas production and distribution, and electric power production and distribution. Many others could have been developed, but these were used primarily because consequence data from accidents and natural disasters (such as Hurricane Katrina) were available. Initial CDCs were developed through consultation at industry meetings described in Chapter 3, and were reviewed and refined by the subject matter experts of the Delphi Group.

1.4.1 Oil and Gas Production

PCS for oil and gas consist of production, refining and pipeline and storage facilities. The process control systems considered include oil extraction process, ballast and balance for floating platforms, pipelines, storage and distribution processes. The primary mode for consequence data are provided by accident data and natural disaster data from Hurricane Katrina. Damages to oil and gas operations have an immediate consequence to the operator, but a short term effect on the market because the oil and gas market have pipelines and storage. The initial effect is speculative, but will be mitigated if no further events happen. The analyses team did not examine multiple related cyber events and the combined consequences. Surveys for provider-developed consequences were not undertaken due to time and cost constraints therefore notional data were used to compute examples.

1.4.2 Electric Power Production

PCS for electric power consist of power generation facilities and transmission facilities. There is no storage in electric power generation. Outages are immediate and costly not only for the provider, but also the customer base. In the long-run, grid capacity may be boosted by other utilities to reduce customer outages if the distribution network is capable of carrying the load. Knock-on effects in the power industry may dwarf the provider costs if the outages are significant. The primary mode for consequence analysis is the Northeast blackout of 2003 and other minor blackouts from available data. Surveys for provider developed consequences were not undertaken due to time and cost constraints therefore notional data were used to compute examples.

2. The Environment

2.1 Cyber Defenses[3]

Consider the security of a house. In this example the house is the system, and the neighborhood is the environment. This security is provided by a set of products such as door locks, window locks, bars on the windows, broken window detectors, motion sensors, and alarms. There are different types of locks and sensors. A five-tumbler lock may take more time to pick or force than a three-tumbler lock. Effective placement of these products depends on the layout of the house. Also, effectiveness depends on the type of lock (5 tumbler locks versus 3 tumbler) and how they are used: if someone does not set the alarm system, forced entry may not be detected until too late. In the end, alarms are tested, sensors are tested, and scenarios of break-ins are run against the system to be sure the risks are understood.

Note that security is not absolute. The amount of security in an information system is restricted by the value of the data or processes: someone does not pay more for the security devices than the data or processes being protected are worth. [Note, however, that an electric utility will suffer some loss when attacked, but their clients may suffer greater loss---does the utility just provide enough protection to counter their own loss?]. Also, security devices tend to make systems harder to use. Banks have lots of money and pay a lot for such things as vaults and armed guards; even so, they are occasionally robbed. The goods in a house typically are of much less value than the money in a bank. Most do not have alarm systems, which cost to install and to provide monitoring; they also make entering and leaving the house more difficult since the alarm must be turned off and on.

Information security products may implement some algorithm, which might differentiate the strength and usefulness of similar products. For example, while many operating systems authenticate users, some do so using passwords and others using smart cards. In a house, while all locks protect against unauthorized entry, some use a key to open, others a combination, and still others a garage door opener. The number of pins may further classify those that use keys.

To evaluate the security of a house, one should start with the overall layout of the house and the placement of the various security products to see if there are unguarded entry points or mismatches between products. Identified weaknesses should be tested to see if

---

[3] The example in this section is derived from (IDA Paper P-4009, "*Evaluation and Review of the National Information Assurance Partnership (NIAP),*" Institute for Defense Analyses, 256 pp., August 2005.

they are exploitable. Also, an overall attack should be tried to determine if there are unexpected weaknesses. However, if the same model of lock is used on each door, one need not try to pick each of them– one is enough. Further, if some laboratory has already tested the lock and determined that it properly incorporates some number of pins and that its case has a specified hardness, the strength of the lock does not need to be tested at all at the house, but rather just that it has been properly installed.

In defending a set of data or a process, we use products, policy, procedures, and people. These elements contain functionality that support confidentiality, integrity, availability, and accountability. However, elements that would not fit this category may very well have an impact on the security of systems. Those products such as word processors, spreadsheets, financial utilities, etc., that are not normally thought of as Information Assurance, (IA), or IA-enabled should none-the-less be candidates for vulnerability testing which is discussed later. Ultimately, an organization is concerned with its entire information infrastructure. This infrastructure consists of a system (the house in the analogy) of many nodes connected by physical, logical, and "air-gapped" networks. The system operates in an environment that is partially controlled and partially uncontrolled (the neighborhood in the analogy). Security is instituted to protect this system from the uncontrolled part of the environment. In order to protect this system, the organization will rely on a variety of products (locks and sensors in the analogy), including devices such as firewalls, intrusion detection systems, and smart card readers, and pieces of software that run on the system nodes, such as operating systems that identify users and limit access to files and browsers that provide secure communication to services. The security of the system depends on the products that are used, the specific security algorithms (such as cryptography) (these are mechanisms in locks and sensors in the analogy), the way that they are incorporated into the system architecture (placement), and the way that they are used. The system developer does not solely rely only on tested products, but also tests his overall system through a process that is designed to quantify the risks inherent in a particular system. Since the products are tested he can worry less about the product details and more about their arrangement, inter-relationships and the end effect.

2.2 Cyber Security

The protection of the information is divided into five primary security services areas: access control, confidentiality, integrity, availability, and nonrepudiation. To this we might add mechanisms (or products) to provide detection and response to violations of the security services. The division of system security principles into standard security service categories is convenient for this description.

Each security service may interact with and depend upon the services. A secure cyber system will include elements of all of these at a level of strength commensurate with the information resources being protected. They may be provided by a combination of products and environmental considerations, such as placing computer resources in a guarded area.

Access Control - In the context of cyber security, access control means limiting access to resources (hardware and software) and information. One of the most common access control mechanism is provided by password logins and/or biometric identification.

Confidentiality - The confidentiality security service is defined as preventing unauthorized disclosure of data (both stored and communicated). Confidentiality services will prevent disclosure of data in storage, or transiting. One of the most common confidentiality mechanisms is the use of cryptography.

Integrity - The integrity security service includes; prevention of unauthorized modification of data (both stored and communicated), detection and notification of unauthorized modification of data, and recording of all changes to data. One of the most common mechanisms for integrity is check sums, or hash algorithms. In some cases independent certification authorities are used.

Availability - Availability is timely, reliable access to data and information services for authorized users. A popular attack is called Denial of Service (DOS), which attempts to make access unavailable.

Accountability - The nonrepudiation security service provides the ability to prove to a third party that the entity did indeed participate in the communication. Some firewalls may refuse communication with parties for which it cannot verify the origin.

Mechanisms such as Access Control are implemented to provide the above functionality. In the context of cyber security, access control means limiting access to resources (hardware and software) and information. One of the most common access control mechanism is provided by password logins and/or biometric identification. In order to provide these basic services, products may provide logs for auditing and tracing events, or even exclusion from access by using accountability. In many cases, forensics on logs will be used to detect unauthorized access and changes to information, provide estimates of losses, and to restore the information to its original integrity.

2.3 The Process Control System

Industrial process control systems have a long history of using unique and proprietary electronics in control applications. As control systems have grown more complex, more information has been needed both from sensors that monitor physical processes and from reporting mechanisms that track systems status. Simple temperature and pressure controls that at one time were handled by thermostats and pressure release valves are now controlled by much more complex nonlinear and conditional functions. This evolution of complex control requirements has led to a rapid growth in the use of information technologies as the solution. Computers and computer networks have become integral parts of process control systems. Unique and proprietary solutions for computers and

network protocols are costly and too inflexible for modern control systems. The process control industry is therefore turning to standard computing and networking technology.

2.3.1 Growth in use of IT

The process control industry has steadily turned to higher levels of automation and connectivity, for competitive advantage and convenience. The computing and network environments assumed for our analysis of risks were derived from examples of corporate computing and process control systems presented at recent electrical power and oil and gas industry information assurance workshops.[4]

Figure 2 shows a number of components that might be found in a typical process control system (PCS) or supervisory control and data acquisition (SCADA) system. Computer workstations and servers are shown connected via a local area network (LAN) or possibly a wide area network (WAN). A key component on the PCS network is the program logic controller, which translates control messages from the workstations and servers into electrical signals that control pumps, valves, and other devices. The program logic controller also translates sensor data into messages sent to workstations and servers. Local devices may be wired directly to the program logic controller. Remote devices may be connected by wireless or other communications. Some of these connections use proprietary communications; others use standard computer network links that connect with another program logic controller at the remote location.

In addition to their process control computers and networks, virtually all organizations have corporate business computers connected by networks. On the corporate side of the house, workstation users run typical business applications such as accounting, personnel, and general word processing, with Internet access for email and World Wide Web services. Some corporate users need information from the PCS side; for example, the accounting department will need production information for billing purposes. On the PCS side, most users run specialized process control applications, but they may also need access to corporate information systems, as well as email and web access.

2.3.2 Move Toward Standard Interfaces

When increasing the automation within an enclave, costs are often reduced by using standard interfaces and applications. A very large number of products are available that use Internet Protocol interfaces and standard application languages such as MODBUS. The advantages and convenience of these standard approaches are enormous. However,

---

[4] These were the electrical power industry Process and Control Systems Forum (PCSF) meeting in March 2007. Oil and gas industry Institute for Information Infrastructure Protection (I3P) Workshop in February 2007.

they carry a price in that the details of how the enterprise communicates and how applications receive and act upon information are available to all, whether in technical publications or courses taught on the open market. This situational awareness makes even the least sophisticated hackers a real threat.

2.3.3 Market and Competition Pressures Among Critical Infrastructure Elements

There is no doubt that Market trends toward automation and reduced costs will continue. Despite this trend, each potential innovation in business practices needs to be evaluated in terms of not only initial cost benefits, but in residual vulnerabilities in systems, and the cost to mitigate apparent or perceived threats.

2.4 IT trends

The IT industry has responded with a number of products that can help mitigate threats to cyber environments. However, they have often done so from an IT perspective and less from an applications perspective. In sensitive process control systems, real-time control of variables and 24 hour operation requirements may prohibit frequent polling and updating of systems. Each application must be considered in light of these factors when dealing with sensitive operations. For this reason, a wide number of configurations are possible and selecting a subset to span the domain is difficult at best.

3. Assessment Modeling Approach

3.1 Modeling Approach and Results of IDA Document D-3309

The initial pilot project undertaken defined a common risk model with common methodologies and approved scales to measure key parameters to accelerate the progress toward the stated goals of the Department in risk assessment activities. The results of this modeling activity were presented in IDA Document D-3309. The report discussed the common risk model and gave examples of its use in the kinetic attack scenario by terrorist threats.

The common risk model presented was:

- **Risk = Consequence*Probability of adversary success/attack* Probability of attack**
  - *Probability of attack* P(a) has a value between 0.0 and 1.0 and is an intelligence function and depends upon data beyond control of the analysis here. The intelligence factor is beyond the scope of this work and we will concentrate on the consequences incurred by an attack which is equivalent to assigning a 1.0 for the likelihood of attack.
  - *Probability of adversary success/attack* P(s/a) = the likelihood of success given an attack takes place. This is a complex function of defenses that are in place and the type of threat = *f (isolation/partition, protection, detection, integrity, availability...).*
  - *Consequence* (C) is the maximum loss under the threat scenario and includes loss of service, loss of data, loss of equipment and loss of life as well as recovery costs in a worst-case scenario. Secondary or chained effects will not be included in the analysis. Each item is converted to a financial figure with loss of each life computed at $7.5M (per reference document).
  - *Risk* (R) is the financial value of tolerating the current cyber levels of protection, given the threat scenarios that are likely and the imminence of an attack.

- *Conditional Risk* (Rc) is the financial value of tolerating the current cyber levels of protection, given the threat scenarios that are likely with an imminent attack likely.

The initial applications of the model concentrated on terrorist attacks using kinetic explosives over a range of infrastructure elements with various forms of defenses in place. A finite number of defensive configurations were mapped and using satellite imagery and other intelligence, defensive configurations for various elements of the infrastructure were determined. Probabilities of success were assigned by subject matter experts and examples were produced that provided a model that effectively supports the decision needs for comparative risk assessment, is credible and understandable, consistent and objective, mathematically defensible, and extensible.

3.2 Data Gathering Through Industry Working Groups

3.2.1 Oil and Gas

Initial contact was made with the Oil and Gas Industry through the Institute for Information Infrastructure Protection (I3P) Control Systems Security Workshop at the Sheraton Houston Brookhollow Hotel, Houston, Texas, February 15-16, 2007. The I3P is a Consortium that includes academic institutions, federally-funded labs and non-profit organizations. The I3P concentrates on cyber security as applied to the oil and gas industry. The I3P functions as a virtual national lab with the ability to organize teams and work groups to address research and policy-related aspects of the vulnerabilities inherent in the information infrastructure. The workshop provided a series of presentations and threat analyses, including hands on threat scenarios and mitigation strategies and well as various forms of accident data that were agreed to be very like a cyber precipitated event. The former aided in the development of defensive configurations and the latter were used for consequence calculations. In some cases, follow-up with individuals was undertaken and such follow-up was beneficial. Of particular note is the work done by New York University[5].

3.2.2 Electric Power Production

Initial contact was made with the Electric Power Industry through the Process Control System Forum (PCFS) annual meeting in Atlanta, Georgia on March 6-8, 2007. The purpose of the PCFS is to facilitate the collaboration of control systems stakeholders to accelerate the design, development, and deployment of more secure control and legacy control systems. Forum participants include international stakeholders from government, academia, industry users, owner/operators, systems integrators; and the vendor

---

[5] Rae Zimmerman, et al., "*Understanding Trends, Causes and Consequences of Failures and Attacks on Oil & Gas Pipeline Infrastructure Systems*," New York University, I3P Process Control Systems Security Workshop, February 15, 2007, Houston, Texas.

community. The PCFS, like the I3P, cuts across a number of control system areas, but concentrates on the electric power industry. The annual meeting provided four-track agendas which covered architecture/design, device/components, requirements/operational considerations, and understanding risk. A number of personal contacts with industry personnel were used to help formulate threat scenarios and defensive configurations. Of particular note were discussions on large scale threat scenarios[6].

3.3 Modified Delphi Approach and Participants

Facilitation of the analysis process was developed using a modified Delphi approach where a number of experts (the Delphi Group) were convened to review and suggest modifications to straw-man work developed by the authors. The process differed from a normal Delphi, in that consensus was sought rather than contention. It was held in abeyance for the normal Delphi process if consensus failed, but it was never needed as consensus was obtained on all issues. The Delphi Group met on four separate occasions and provided reviews of this document. A list of Delphi participant's and their relevant experience is provided in Appendix C.

3.4 Validation Process

Several of the preceding steps were subjected to validation at a workshop attended by outside subject matter experts not previously associated with, or otherwise exposed, to the project. The validators were asked, primarily, to assess the estimates produced by the Delphi group were not demonstrably false. Since these are *subjective* estimates, the validators were not asked to certify that the estimates were correct. The estimates were considered to not be demonstrably false if they exhibited logical consistency and coherence, and the rationales presented for making the estimates were reasonable and logically supportable. Appendix E contains relevant working definitions used in the validation process, and biographies of the participants in the validation workshop. The participants were made available to IDA by DHS sponsors. Two were supplied to DHS by Oak Ridge Associated Universities (ORAU) without direct involvement by either DHS or IDA. Another was supplied by DHS. DHS and ORAU each also supplied one discussant for the validation workshop.

Secondarily, the validators were asked to validate: (1) the appropriateness of extending to the analysis of defense against cyber threats, the Common Risk Model, (CRM), methodology as developed for analysis of defense against physical attacks; and (2) the attack paths and cyber defense configurations that were developed.

---

[6] Personal conversations, with Joe Weiss PE, CISM, Applied Control Solutions, LLC, Cupertino, CA, on March 14 and March 15, 2007.

The validation process differs from a typical external review. In part, it mirrors aspects of the estimation process. The participants were given background material to read before the meeting. This material was then briefed in detail at the beginning of the meeting. The specific attack paths, defensive configurations, estimation rationales and estimation results were not presented until the workshop, when they were discussed in as much detail as the validators thought necessary to support their deliberations.

The validation team:

- Supported the application of the Common Risk Model methodology to cyber attacks
- Accepted the three defined threat levels, but noted that this list was far from comprehensive and suggested that others be added
- Suggested the addition of two more CDCs , noted that the CDCs "cover" the space of defenses from least capable to most capable, but do not necessarily "span" the space of all relevant possibilities, and agreed that the method that was employed to build the CDCs is otherwise (and generally) reasonable
- For future analysis, they suggested:
  - Adding cyber response team as part of the defense
  - More detailed analysis to understand the possibility of interference among defensive measures
  - The use of multiple SME teams to conduct estimates and the development of a process for combining multiple estimates
- Supported the current estimates as sufficient at this stage in the overall process
  - *Taken under advisement for future work*
- Validated the estimates as displaying coherence and cohesion, and being based on sound, supportable rationales

The validators agreed that the work done to-date was sufficient for the stated purposes and formed a sound basis for revising, re-estimating, and adding additional estimates as new information and analysis becomes available.

4. Cyber Defensive Configurations

4.1 The PCS (Functionally)

There is no single representation of a process control system. In fact, it may masquerade by many names including Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS) and a number of other names. It is characterized by the collection manual and automated instruments and controls that monitor a process. Figure 1 shows that other control system(s) may be imbedded within the overall control system.

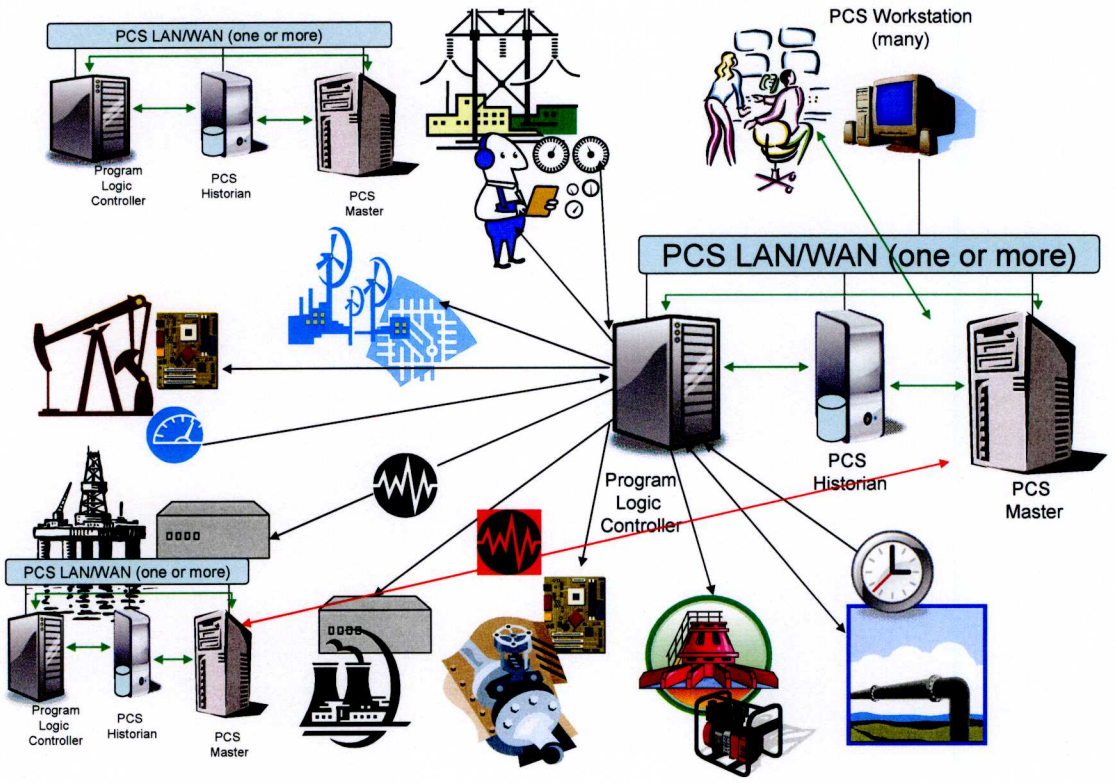

Figure 1. Process Control System

As shown, the oil platform has a ballast control system which is secondarily controlled by the overall production control system. The figure also shows many people are involved in the process, but more and more systems are automated through IT. This includes the aspects of control as well as instrumentation. Almost all PCS systems contain a Master that sends commands to the Logic Controller and a Historian so that a person or automated computer process can monitor progress over time. Defending this system, from a cyber sense is defending the network that is the backbone for services.

4.2 Corporate/Marketing/PCS Common Elements

Additionally, the corporate requirements for network operations have a number of common elements that can be developed. Each Corporation has a need to monitor operations, maintain a web presence, maintain e-mail, and perhaps market their products in real-time or near real-time. Figure 2 shows this basic structure. Common elements include a domain controller, servers for web and e-mail and many workstations at all levels for marketing, administration, and PCS control. The security aspects of these and the other figures will not be discussed until we get to the cyber defensive configurations (CDCs) section. There are many complicated issues, but for now, we will restrict the discussion to functional arrangements.

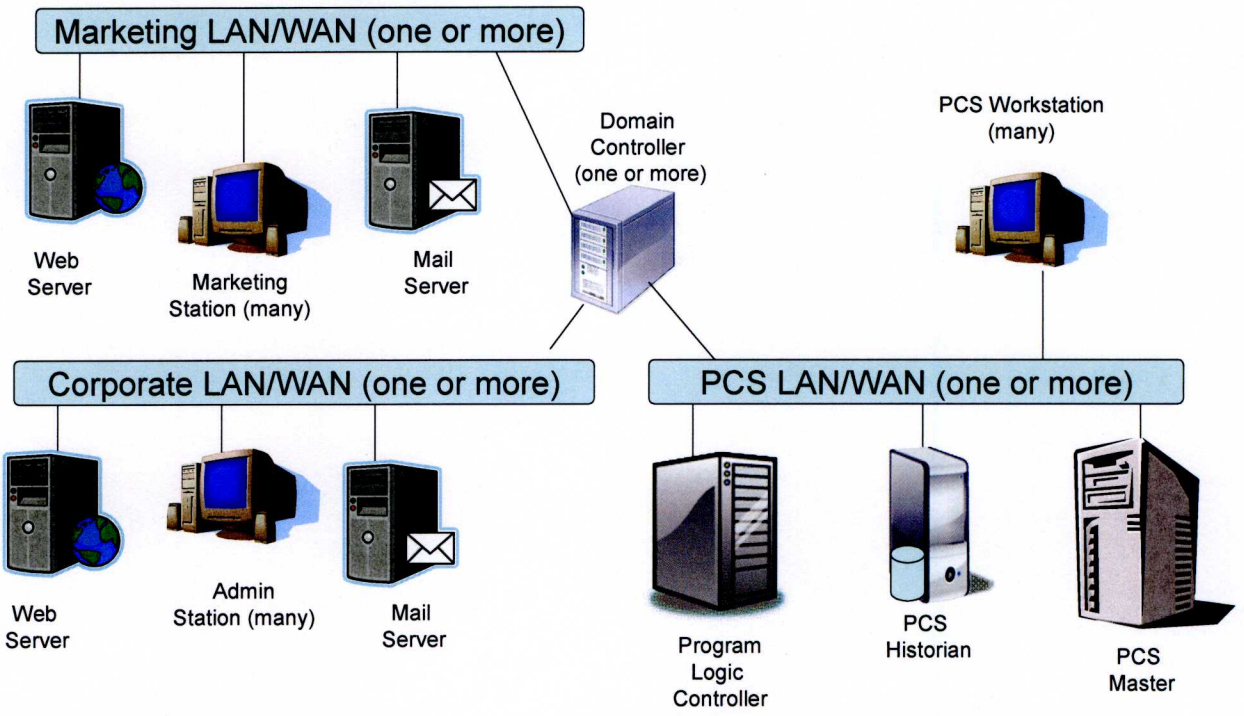

Figure 2. Basic Elements of the Corporate Network When PCS Elements are Present

4.3 Basic types of LAN/WAN in the PCS

Most PCS IT systems can be represented by three separate cases which have developed from the increased automation sought. These configurations may or may not have developed from security considerations, although we will see that they have an impact on security. All of these configurations will exist in the vast array of critical infrastructure. Other configurations may also exist, and it is hoped that their numbers are small and

specialized, so that the bulk of critical infrastructure elements can be analyzed based upon these basic configurations. These are delineated below.

4.3.1 Integrated

In an integrated environment, the PCS is one more component of a corporate network. All components are physically tied together through an Ethernet cable or other

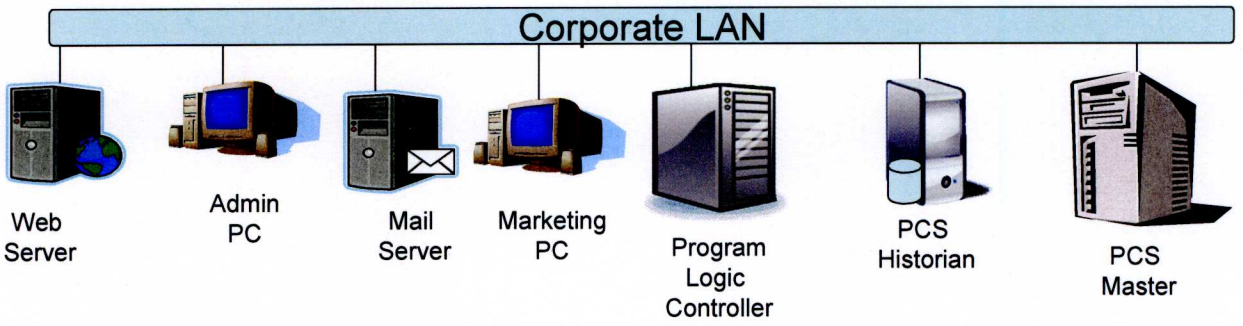

Figure 3. Integrated PCS

networking approach. This is shown in Figure 3. From a corporate standpoint this is the most convenient and easiest to implement, although the most vulnerable. Such PCS may be a small chemical plant, food processing plant or a single site where all aspects of the service are provided such as a small rural electric company.

4.3.2 Separated

In a separated environment, it is recognized that the PCS needs to be separated from the overall network. This is often done to prevent corporate or marketing from directly affecting the PCS system which may have very stringent real-time requirements. In order to do this, there is a second historian set up with some refresh rate that is consistent with corporate needs and provides a near real-time picture of the operation. Though separate networks, they are very much logically connected through the update of the admin historian which is used by the corporate and marketing sides of the house. This also has the added benefit of improving the overall security of the PCS System. This configuration is shown in Figure 4. It might be found in an intermediate size water facility or electric power operation.

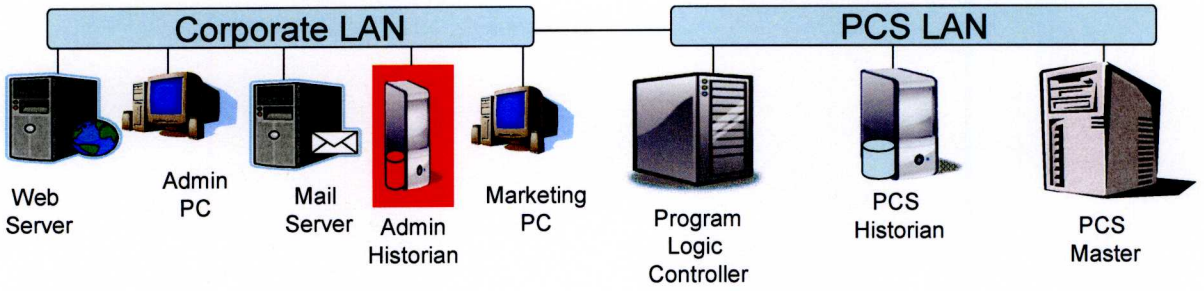

Figure 4. Separated PCS

4.3.3 Isolated

The third type of configuration involves an isolation approach. This may be done from a safety configuration standpoint or by legal requirements because the risk of being connected to the corporate network is just too great. Figure 5 shows this type of configuration

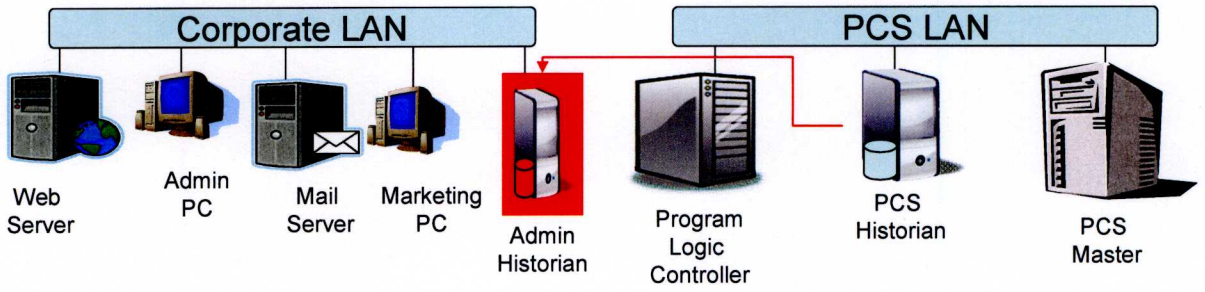

Figure 5. Isolated PCS

In this configuration, the logical link is broken and a one-way update to the admin historian is undertaken or a separate sensing network is used for the admin historian. This can be done several ways from an IT perspective, but for now, consider manual porting of the data from the PCS side to the corporate side. This increases the lags in the picture presented to the corporate side but can still be near real-time. One example of this arrangement might be a nuclear power plant, but it could also be found in a remote mining or oil production facility, or in a high security environment.

4.4 Approach to Enumeration of CDCs for PCS Systems

There exist a number of things that can be done to improve security in each one of the configurations listed. For example, installing firewall, ant-virus, anti-spam, restricted access, etc. Additionally there are some best practice issues that need to be developed either within the configurations or external to them. After many trial and error approaches the process was to develop an increasing level of security within each of the basic categories as shown in Figure 6. This would be done by using the following basic building blocks:

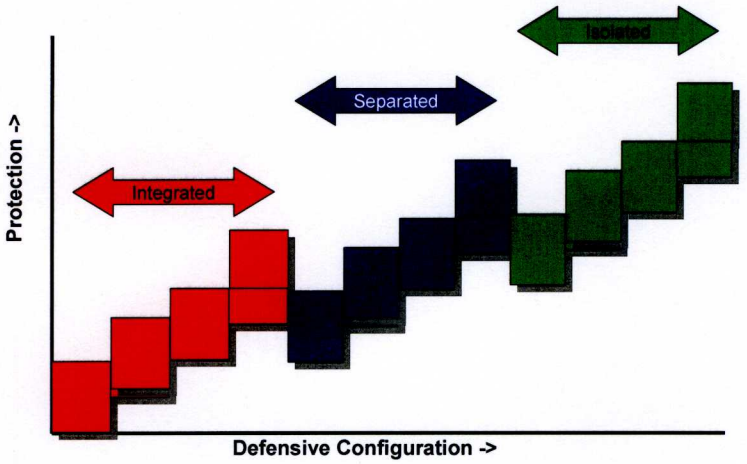

Figure 6. Defensive Configuration Buildup

A. **Firewall and anti-virus/spam** – the first line of defense and probably the easiest for a corporation to implement. It implies that some form of identification and authorization are in place. These may range from simple passwords to biological identification. As with all elements in this analysis, the strength of function associated with firewalls and identification are assumed to escalate with the overall security posture, obviating the need to account for these details.

B. **DMZ for internet and intrusion detection** – considerably more difficult to implement, requiring more hardware and sophistication. The **DMZ** is essentially a set of firewalls that act as one-way valves to keep hazardous activities contained where they can be monitored and prevented from spreading. **Intrusion Detection** – Hardware and software dedicated to checking the information flow for anomalous behavior that might indicate a cyber intrusion. The simplest form of this is the honeypot, consisting of a work station on the net that contains files that are attractive looking to an intruder, and software that notifies a security individual when these files are accessed. Under ordinary circumstance, the honeypot is not accessed by trusted or untrusted personnel in the IT environment. An important concept here

is that indications of intrusion are met by a response team that will do forensics and cleaning of systems. Many attacks can be discovered in the early phases before serious damage can occur.

C. **Actively managed security** (training, audits, updates, log reviews) – a change in corporate philosophy making security everybody's business. This building block is not only essential to a secure computing environment, but bolsters the response-team approach described above.

D. **Defense in-depth** - with additional firewalls and intrusion detection at key points - includes PCS encryption and authentication. This building block adds extra impediments to an attacker by making the attacher overcome additional obstacles. It also provides a point of awareness for intrusion detection systems.

E. **Insider Protection** (Personnel Screening and Monitoring) – a measured amount of paranoia is required at this level. However, the insider threat is the most difficult to stop.

4.5 Applying the Building Blocks

The above building blocks were applied in an escalating security environment with each block building upon the previous work. As each block of protection is added, it is assumed that previous blocks are updated and strengthened to match the overall security posture. Figure 7 illustrates the buildup to the defensive configurations.

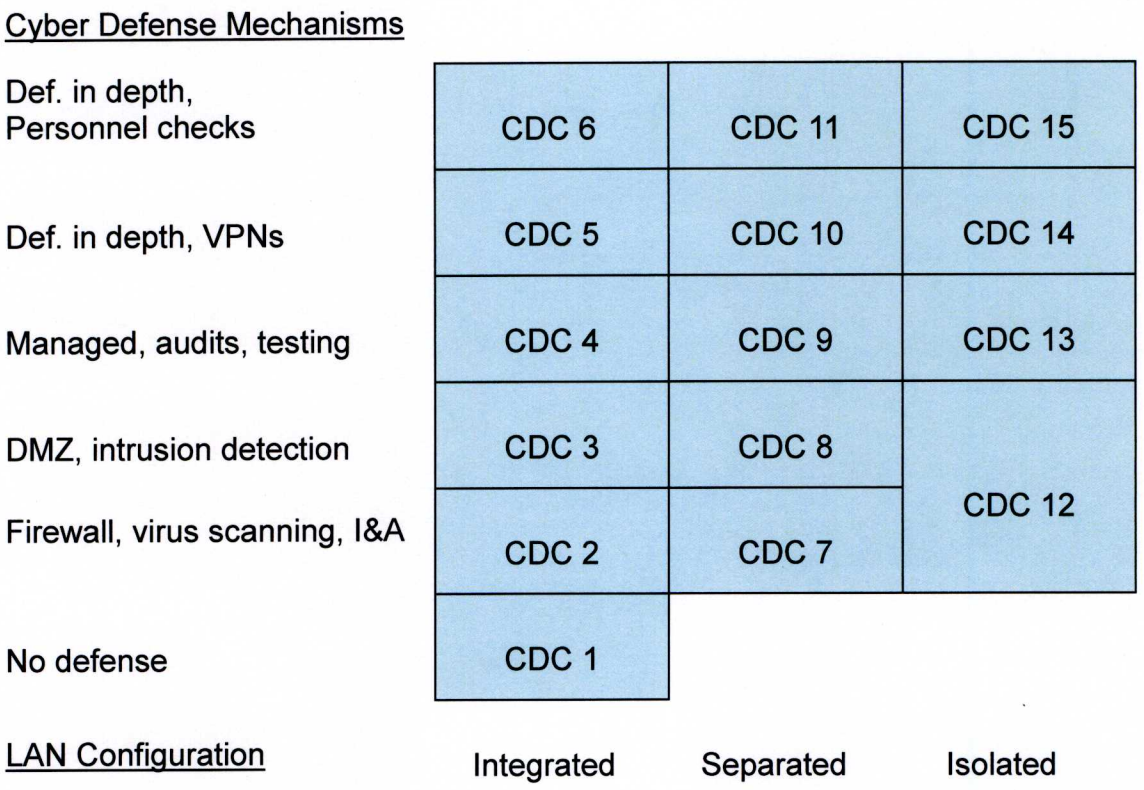

Figure 7. CDC Buildup

4.6 The CDCs for PCS Systems

The 15 configurations for the PCS defensive configurations are derived from the approach presented in Table 1.

Table 1. Defensive Configurations

	Firewall Anti-Virus	DMZ intrusion detection	Actively managed	Defense in depth	Insider Protection	Comments
Integrated						
CDC1						Unprotected LAN
CDC2	x					Baseline Protection
CDC3	x	x				Enhanced Protection
CDC4	x	x	x			Actively Managed
CDC5	x	x	x	x		Defense in depth
CDC6	x	x	x	x	x	Additional Insider Protection added
Separated						
CDC7	x					Baseline protection
CDC8	x	x				Enhanced protection
CDC9	x	x	x			Managed protection
CDC10	x	x	x	x		Defense in depth
CDC11	x	x	x	x	x	Additional Insider Protection added
Isolated						
CDC12	x	x				Physically and logically separated version of CDC7
CDC13	x	x	x			Physically and logically separated version of CDC8
CDC14	x	x	x	x		Physically and logically separated version of CDC9
CDC15	x	x	x	x	x	Additional Insider Protection added

In Chapter 5, after a description of the threat, Delphi developed probabilities of success given an attack.

4.6.1 Cyber Defensive Configuration 1 - Integrated

The first set of defensive configurations (6 in total) is for an integrated corporate and PCS network. This defensive configuration is included as a baseline for no protection. There are no cyber attack mitigations in place. Hopefully no part of the critical infrastructure is at this position in today's environment. The basic LAN configuration is shown in Figure 8. This configuration also serves as an anchor point making it the easiest to attack. There are four basic ingress paths. From the outside, an attacker can enter through the web portal or through the communications with the program logic controller. It can be attacked from anywhere on the inside, but for classification purposes we catalogue attacks from the corporate insider or the PCS insider.

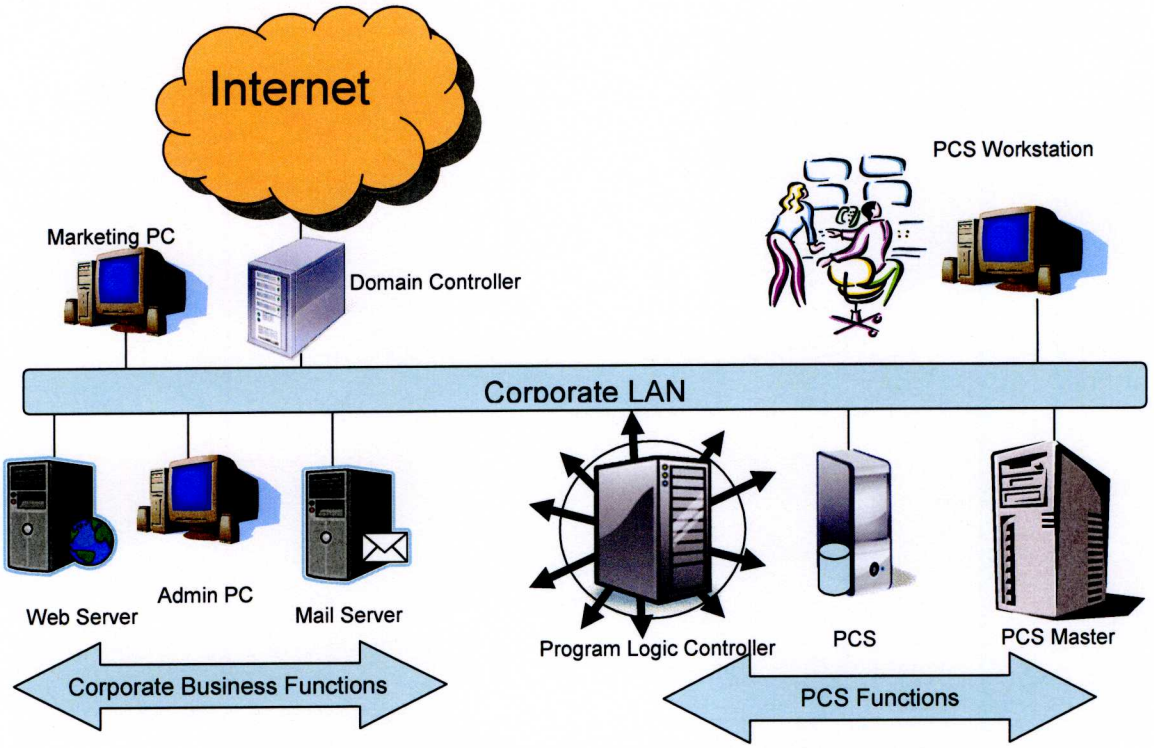

Figure 8. Cyber Defense Configuration 1

4.6.2 Cyber Defensive Configuration 2 – Integrated

For defensive configuration 2 we have added a standard firewall along with anti-spam and anti-virus software. This is the configuration of most home computers and probably a few networks. This configuration is shown in Figure 9. In the figure, we have highlighted the changes from the last configuration by placing a box around the items. There are four basic ingress paths as before, but additional obstacles have been raised. From the outside, an attacker can enter through the web portal, but through a firewall[7] that offers some protection, and the use of common viruses is mitigated with anti-spam. The attacker can also enter through the communications with the program logic controller. It can be attacked from the inside, by the corporate insider or the PCS insider.

---

[7] In the interest of simplicity we have not differentiated firewalls by type. Obviously some are more effective than others and we would assume that an initial implementation would handle flow control by a simple white-list/black-list approach. As defenses are upgraded, it is also assumed that more effective types of flow control may be initiated.

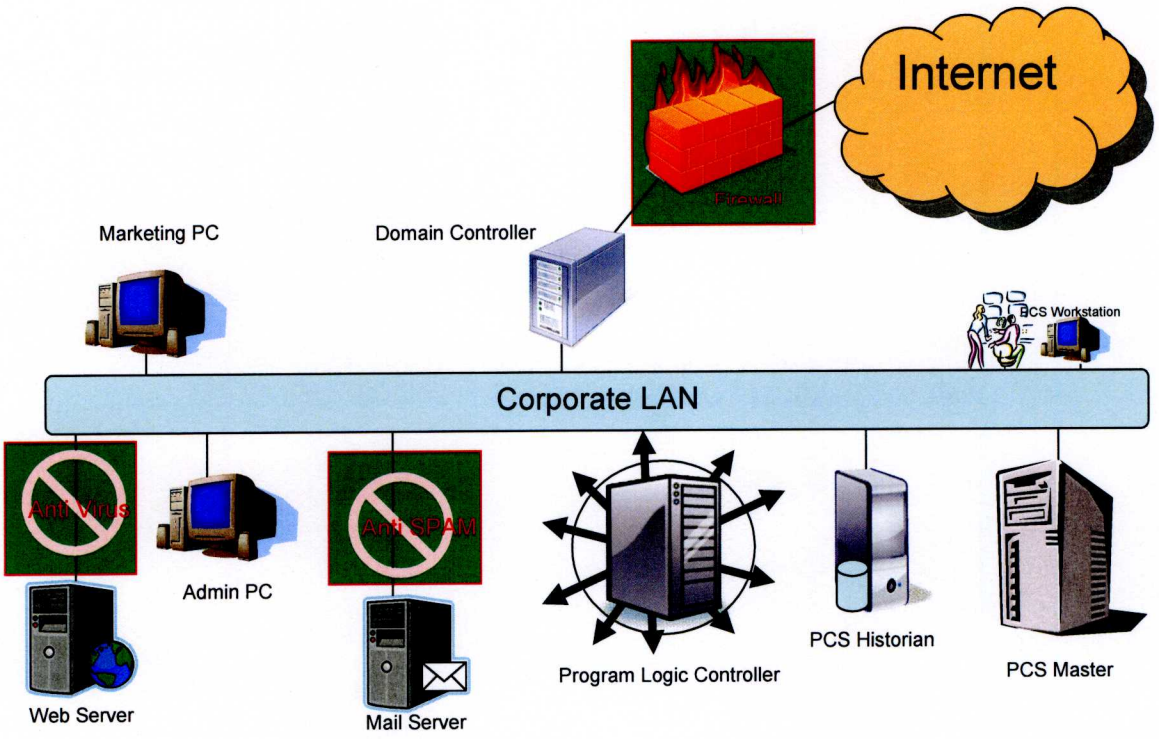

Figure 9. Cyber Defense Configuration 2

4.6.3 Cyber Defensive Configuration 3 – Integrated

For defensive configuration 3 we have added a demilitarized zone (DMZ) to provide some isolation from the net. We have also added a basic intrusion detection[8] capability. This is the configuration expected for most corporate networks. This configuration is shown in Figure 10. In the figure, we have highlighted the changes from the last configuration by placing a box around the items. There are four basic ingress paths as before, but additional obstacles have been raised. From the outside, an attacker can enter through the web portal, but through a firewall into a demilitarized zone where access is precisely controlled. The use of white-list only for the corporate side is common. The attacker here must breach two different firewalls, while not preventative, it does add difficulty. The attacker can also enter through the communications with the program logic controller. It can be attacked from the inside, by the corporate insider or the PCS insider.

---

[8] We have added a honeypot to the notional intrusion detection, in that it is inexpensive and effective. The honeypot can be any piece of equipment (old retired work-station, for example) that is configured with attractive data, and not used by anybody internally. Access provides an alarm that is an intrusion, a violation of policy or a mistake. – The canary in the mine. An array of escalating capabilities in intrusion detection is available and we assume that these will be upgraded as defensive postures are enhanced.

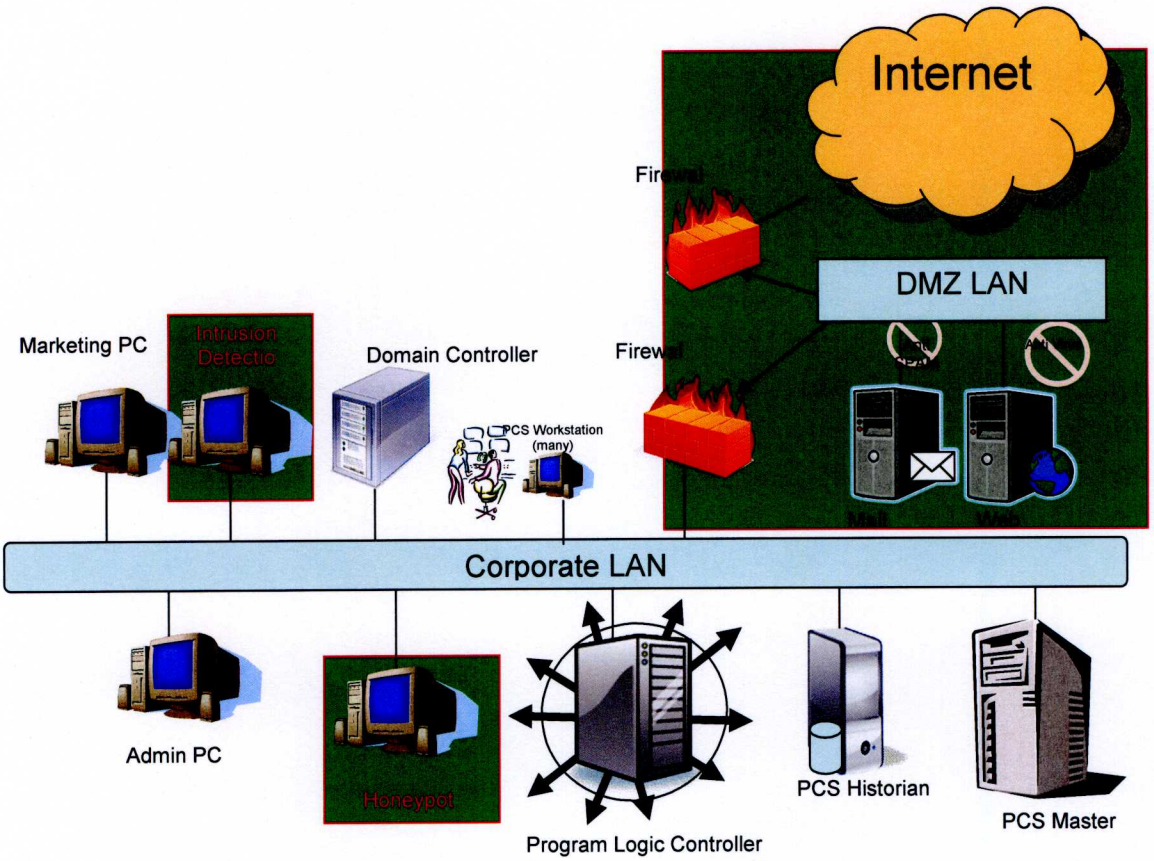

Figure 10. Cyber Defense Configuration 3

4.6.4 Cyber Defensive Configuration 4 – Integrated

For defensive configuration 4 we have added a managed security package that includes:

- Configuration Audits
- Vulnerability Testing
- Periodic Log Reviews
- Personnel Training and Awareness programs
- Automated Updates to Systems and Security Applications

This configuration is a step above those expected for most corporate networks. There are four basic ingress paths as before, but attacks cannot be based on vulnerabilities with known fixes. The training and awareness may partially mitigate the insider threat.

4.6.5 Cyber Defensive Configuration 5 – Integrated

For defensive configuration 5 we implement a defense-in-depth security package that includes:

- Placing of Firewalls at critical internal locations (especially the PCS)
- Placing of additional intrusion detection at critical internal locations.
- Encryption and authentication of all communications

This is the configuration expected for high security corporate networks. There are four basic ingress paths as before, but attacks cannot be based on vulnerabilities with known fixes. The four paths of intrusion exist, but with greater difficulty. The attacker can still enter through the communications with the program logic controller, encryption and authentication making this difficult. It can be attacked from the inside, by the corporate insider or the PCS insider.

4.6.6 Cyber Defensive Configuration 6 – Integrated

This configuration adds the following protections:

- Personnel Background Checks
- Personnel Activity Monitoring
- Enhance Intrusion Detection (either monitored or daily log reviews, etc.)

The bullets above deal directly with the insider threat and the latter bullets above with the communications through the logic controller. There are four basic ingress paths. The attacker can enter through external communications with the web and/or the communications with the program logic controller. It can be attacked from the inside, by the corporate and/or the PCS insider.

4.6.7 Cyber Defensive Configuration 7 – Separated

At some point in the security upgrade process it is realized that only so much can be done with an integrated network. The first step is in separation of the PCS system from the corporate LAN. In moderate to large enterprises this may have already happened for geographic or management reasons. The baseline case here includes the basic protections of CDC 2. Additionally, to achieve the separation, two elements are normally added. The first is a mirror of the PCS Historian. We call it the admin historian, and it may have various names in the PCS systems. Its purpose is to mitigate the need for corporate and marketing to directly communicate with the PCS system. It is a periodic update of the data used to control the system and provides a near real-time look for corporate executives and marketing types. The latter is extremely important in the electric industry where we have near real-time sales and purchases of grid power to meet customer

demand. There is a firewall placed at the logical connection point that is set to allow the update of the admin historian and little else. There are four basic ingress paths as before, but additional obstacles have been raised. From the outside, an attacker can enter through the web portal, but through a firewall into the corporate LAN where a second, and more restrictive firewall must be breached. The attacker here must breach two different firewalls, while not preventative, it does add difficulty. The attacker can also enter through the communications with the program logic controller. It can be attacked from the inside, by the corporate insider (although, still with the breach of one firewall) or the PCS insider. The basic configuration is shown in Figure 11. The remaining configurations for the separated case mirror the configurations for the integrated case.

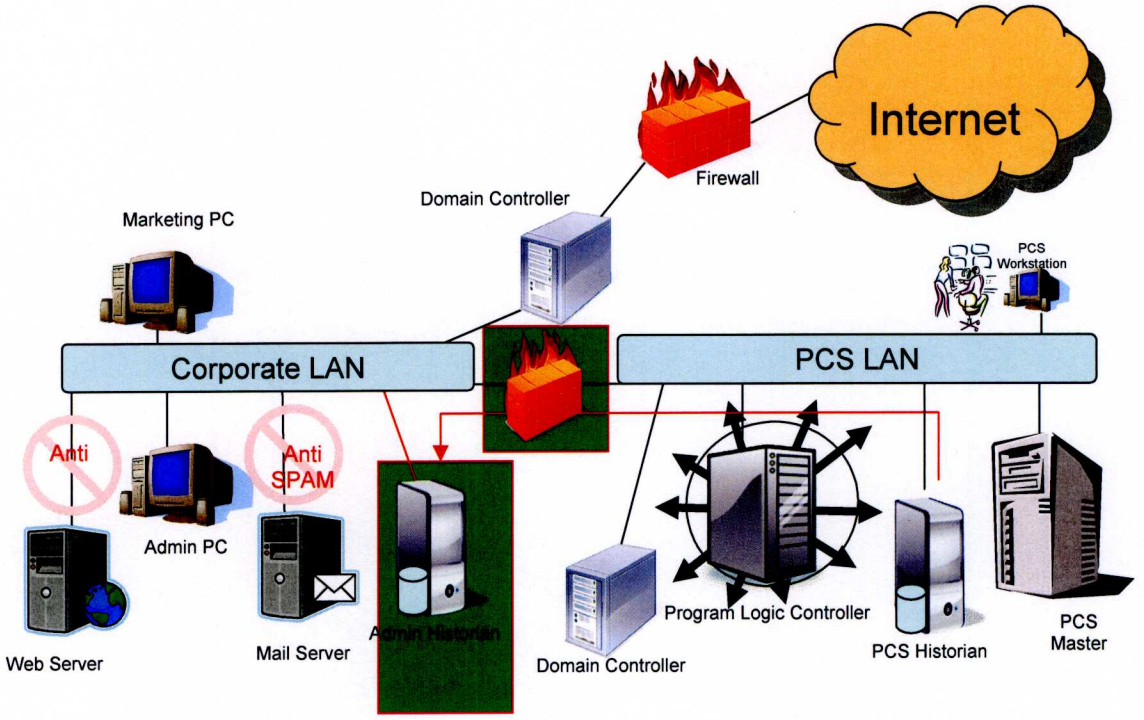

Figure 11. Cyber Defense Configuration 7

4.6.8 Cyber Defensive Configuration 8 – Separated

This configuration mirrors CDC 3 for the integrated case. For defensive configuration 8 we have added a demilitarized zone (DMZ) to provide some isolation from the net. We have also added a basic intrusion detection capability. This is the configuration expected for most corporate networks, except this includes a separated PCS. Corporate networks may have this feature also for reasons of geography or administration. There are four basic ingress paths as before. From the outside, an attacker can enter through the web portal, but through a firewall into a demilitarized zone where access is precisely controlled. To reach the PCS, a third firewall must be breached. The attacker here must breach three different firewalls, while not preventative, it does add difficulty. The

attacker can also enter through the communications with the program logic controller. It can be attacked from the inside, by the corporate insider or the PCS insider.

4.6.9 Cyber Defensive Configuration 9 – Separated

This configuration mirrors CDC 4 for the integrated case. For defensive configuration 9 we have added a managed security package that includes:

- Configuration Audits
- Vulnerability Testing
- Periodic Log Reviews
- Personnel Training and Awareness programs
- Automated Updates to Systems and Security Applications – in the separated case, a push update may be allowed as an exception to the firewall between the corporate LAN and the PCS.

This configuration is a step above those expected for most corporate networks. There are four basic ingress paths as before, but attacks cannot be based on vulnerabilities with known fixes. The training and awareness may partially mitigate the insider threat.

4.6.10 Cyber Defensive Configuration 10 – Separated

This configuration mirrors CDC 5 for the integrated case. For defensive configuration 10 we implement a defense-in-depth security package that includes:

- Placing of Firewalls at critical internal locations (especially the PCS)
- Placing of additional intrusion detection at critical internal locations
- Encryption and authentication of all communications

This is the configuration expected for high security corporate networks. There are four basic ingress paths as before, but attacks cannot be based on vulnerabilities with known fixes. The four paths of intrusion exist, but with greater difficulty. The attacker can still enter through the communications with the program logic controller, encryption and authentication making this difficult. It can be attacked from the inside, by the corporate insider or the PCS insider.

4.6.11 Cyber Defensive Configuration 11 – Separated

This configuration mirrors CDC 6 and adds the following protections:

- Personnel Background Checks

- Personnel Activity Monitoring
- Enhance Intrusion Detection (either monitored or daily log reviews, etc.)

The first two deal directly with the insider threat and the latter with the communications through the logic controller. There are four basic ingress paths. The attacker can enter through external communications with the web and/or the communications with the program logic controller. It can be attacked from the inside, by the corporate and/or the PCS insider.

4.6.12 Cyber Defensive Configuration 12 – Isolated

At some point in the security upgrade process it is realized that only so much can be done with a separated network. The next step is in isolation of the PCS system from the corporate LAN. This type of isolation would occur for safety or security reasons, like in a nuclear power plant. The baseline case here includes the basic protections of CDC 3. Additionally, to achieve the isolation, a clean separation must be achieved. Isolation is particularly important for the admin historian which may have its own sensor network, or be manually updated. The latter may reduce the real-or near-time performances. There are two basic ingress paths on the PCS side. The attacker can enter through the communications with the program logic controller. It can be attacked from the inside, by the PCS insider. The basic configuration is shown in Figure 12. The configurations for the isolated case mirror the configurations for the separated case, except in the last configuration which affords additional insider protection.

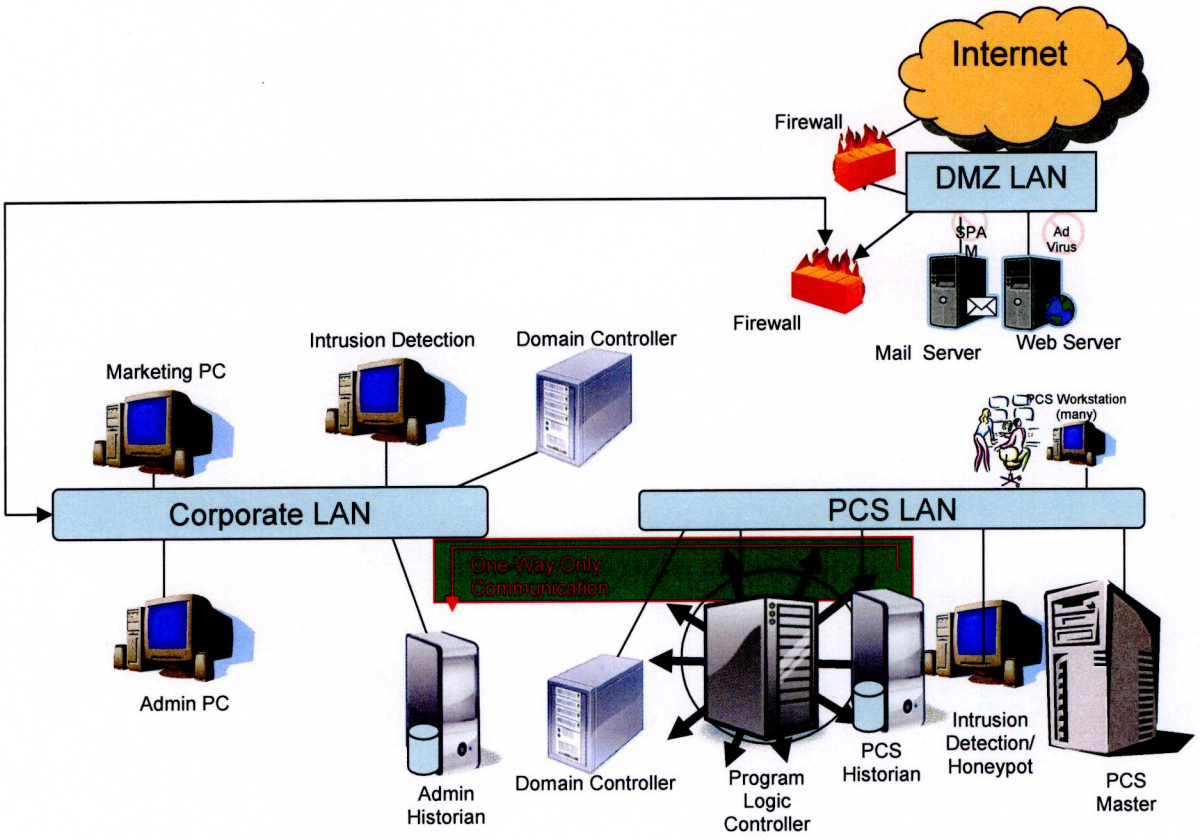

Figure 12. Cyber Defense Configuration 12

4.6.13 Cyber Defensive Configuration 13 – Isolated

This configuration mirrors CDC 4 for the integrated case and CDC 9 for the separated case. For defensive configuration 13 we have added a managed security package that includes:

- Configuration Audits
- Vulnerability Testing
- Periodic Log Reviews
- Personnel Training and Awareness programs
- Automated Updates to Systems and Security Applications – in the isolated case, a push update may not be allowed and this may have to be done by importing a sanitized CD to the system (commonly called "air-gap").

This configuration is a step above those expected for most corporate networks. There are two basic ingress paths on the PCS side. The attacker can enter through the

communications with the program logic controller. It can be attacked from the inside, by the PCS insider. The training and awareness may partially mitigate the insider threat.

4.6.14 Cyber Defensive Configuration 14 – Isolated

This configuration mirrors CDC 5 for the integrated case and configuration 10 for the separated case. For defensive configuration 14 we implement a defense-in-depth security package that includes:

- Placing of Firewalls at critical internal locations (especially the PCS)
- Placing of additional intrusion detection at critical internal locations
- Encryption and authentication of all communications

This configuration is expected for high security corporate networks. There are two basic ingress paths on the PCS side. The attacker can enter through the communications with the program logic controller. It can be attacked from the inside, by the PCS insider.

4.6.15 Cyber Defensive Configuration 15 – Isolated

This configuration mirrors cases CDC 6 for the integrated and CDC 11 for the separated and adds the following protections:

- Personnel Background Checks
- Personnel Activity Monitoring
- Enhance Intrusion Detection (either monitored or daily log reviews, etc.)

The first two deal directly with the insider threat and the latter with the communications through the logic controller. There are two basic ingress paths on the PCS side. The attacker can enter through the communications with the program logic controller. It can be attacked from the inside, by the PCS insider.

4.7 CDCs for Corporate LAN

In general combined effects were not examined; however, the corporate LAN is a special case of the integrated configuration and was developed to cover the case for those who may wish to do an analysis of combined effects. The case of the corporate LAN was not examined in detail, and these computations assume that the PCS Master is the target for an attacker. However, the integrated LAN data can be used as a first approximation. The CDCs that apply to the integrated case are shown in Table 2.

Table 2. Corporate LAN Configurations

	Firewall Anti-Virus	DMZ intrusion detection	Actively managed	Defense in depth	Insider Protection	Comments
Integrated						
CDC1						Unprotected LAN
CDC2	x					Baseline Protection
CDC3	x	x				Enhanced Protection
CDC4	x	x	x			Actively Managed
CDC5	x	x	x	x		Defense in depth
CDC6	x	x	x	x	x	Enhanced Defense in depth

4.8 Survey Questions For Establishing Defensive Configurations for PCS Systems

At this point, questions remain to determine which CDC most closely resembles any given infrastructure. A list of questions was developed that provided coverage of the CDCs and a unique set of answers for each CDC[9]. They are listed below:

1. Do PCS/SCADA systems operate on networks that are physically tied to other corporate or business computer systems? - physically tied means by wire to the network or to a server on the network?

2. Do PCS/SCADA systems have access to email, corporate business file systems, or internet web services?

3. Are all computer systems and networks protected from the internet by a firewall?

4. Are internet application systems and networks protected by virus and spam filters?

5. Are computer systems and networks protected by intrusion detection systems?

6. Are computer systems and networks protected from the internet by a double-firewalled demilitarized zone (DMZ) that separates email and external web servers from the internal network?

7. Are software updates and patches automated or at least managed as a business process?

---

[9] The list of questions include penalty items for best practices (questions 16-19 and to some extent 2). These are discussed in section 6.4

8. Are configurations of computer systems and networks audited on a periodic basis?

9. Are computer systems and networks tested for vulnerabilities on a periodic basis?

10. Are computer system access logs and network traffic logs reviewed on a periodic basis?

11. Are firewalls or virtual private networks (VPNs) used internally to separate sensitive business functions?

12. Are authentication mechanisms used to verify the authenticity and integrity of information exchanges on PCS/SCADA networks?

13. Are firewalls used to separate PCS/SCADA networks from other corporate or business networks?

14. Are PCS/SCADA networks effectively "air gapped" to isolate them from other corporate and business networks?

15. Are all PCS/SCADA system operations and maintenance staff screened for dependability, integrity, loyalty, and trustworthiness?

16. For any PCS/SCADA systems that are connected via wireless communications, is the integrity of these transactions protected by appropriate encryption techniques?

17. Are USB devices allowed to be used on any PCS/SCADA systems?

18. Are PCS/SCADA systems and networks provided physical protection equal to the worth of the protected resources?

19. Are Corporate systems and networks provided physical protection equal to the worth of the protected resources?

20. Do all PCS/SCADA system operators use their own accounts and passwords?

21. Are user accounts and passwords required to be stored in some form of cipher (other than plain text)?

22. Are default accounts and passwords always required to be changed?

23. Are password complexity rules enforced?

24. Are passwords required to be changed periodically?

25. Are scripts, macros, patches and other software developed within the organization required to be examined for well known vulnerabilities, such as buffer overflows?

26. Are all unnecessary services required to be disabled or removed from systems?

27. Are Intrusion Detection Systems required to be set to monitor for disabled ports and services?

28. Are firewalls required to be set to deny connections by default?

While these 28 questions cover the set of CDCs, responses do not necessarily uniquely identify one configuration. This is discussed further in Chapter 7.

5. Threat Scenarios

5.1 General

Three threat scenarios were postulated for each of the 15 cyber defense configurations. These involve a range of threats by attribute and are typified by spot terrorist attack, criminal extortion, or well-organized terrorist or nation-state attack.

5.1.1 Cyber Attack Vectors for the Enumerated CDCs

External attack is defined as an attack from outside the LAN/WAN system. For the PCS this would either be through the web or e-mail interface or through one of the many interfaces to the Program Logic Controller (PLC). Legacy systems that connect to the PLC are often specialized (even proprietary) format and difficult to use as an attack point, but modernization of these systems by using a wide variety of IP type interfaces are more vulnerable. The goal of any such attack is control of the PCS Master, but successful attacks may require less (such as changing set points within the PLC).

Insider Attack is defined as any attack that is generated or assisted by personnel inside the system (having access to some aspect of the LAN/WAN). Again the ultimate goal is control of the PCS Master.

5.2 Threat1 – T1

The first threat scenario involves a small group of individuals with moderate cyber capabilities and a limited time-frame to execute a plan, either through coordination with other events or impatience. This group has a fair amount of expertise to penetrate networks and disrupt computer systems. The tools available include those commonly available on the internet and through "Black-Hat"[10] contacts. The motivation is to disrupt or shut down electrical power or oil or gas distribution as a political, social, or religious statement. The group may also include disgruntled employees. The objective is to cause damage to the particular utility and inflict injury on the population it serves. These groups are more likely to time their attacks to coincide with bad weather such as a winter cold spell to expand the effects of a power outage. We assume such groups are formed and dissolved rather quickly. This limits the amount of time they have to spend on network surveillance and attack planning. They are less concerned about being identified; in fact, some may openly claim responsibility. The group is expected to

[10] Black-Hat organizations are groups of hackers that share information through electronic means and through annual meetings, typically held in Las Vegas, NV.

disband immediately after a successful attack. This scenario is typified by a spot terrorist attack, but could be any of the groups mentioned above.

5.3 Threat2 – T2

The second scenario involves individuals with moderate cyber capabilities with the advantage of time and timing. The tools available include those commonly available on the internet and through "Black-Hat" contacts. The motivation for attack is money through extortion. The extortionist's objective is the money, not disrupting their victim's operations. The group will threaten cyber attack to disrupt or shut down control system capabilities unless a sizeable ransom is paid. They would be just as happy to be paid and not attack the target network. If they are not paid, though, they have a fair amount of expertise to penetrate networks and disrupt computer systems. They will take care not to be identified and try to ensure that attacks cannot be traced back to their source. Their objective is to teach their victim a lesson so their extortion demands will be paid the next time they threaten. It is perfectly acceptable to the extortionist if the attack looks to the public like an accidental disruption of service. This threat is typified by a criminal extortion, but may also be perpetrated by a disgruntled or greedy employee.

5.4 Threat3 – T3

The third scenario involves an attack to cause extensive damage to major utility resources with long lead-time repairs and costly restoration. Such attacks are assumed to be beyond the means and technical abilities of isolated terrorist cells. The financial damage they cause to the utility also goes beyond the extortionist's objectives. The groups here are assumed to be well funded, have extensive expertise in network and computer technologies, and have adequate time for network surveillance and attack planning. For example, these groups would have the resources and time to set up a model network that emulates their target environment in a laboratory setting, where they could practice attack techniques. They are also likely to have the time and resources to plant one or more members of their group as employees inside the target organization. Insider attacks are the most challenging threats for cyber defense. These groups may be typified by dedicated and resourced terrorist cells, and/or nation-state operations.

6. An Attack Given Enumerated Probabilities of Success

6.1 Delphi Deliberations

Given that process control systems rely increasingly on standard computers and networks, and experience has shown that these systems have vulnerabilities that can be exploited to disrupt operations, an attacker, given enough time and resources, will almost certainly be able to succeed. The problem from the attacker's point of view is that they are time and resource constrained, and their probability of success is reduced accordingly. The problem we posed to the Delphi Group was to rate the attackers' probability of success, based on the descriptions of the attack scenarios and the time and resource constraints implied by those operating conditions. The convening of the Delphi Group for the first of four occasions brought the experts together for a review of the work, and a lively discussion of probabilities and likelihoods together with attack scenarios. Each of these was refined over subsequent meetings of the Group. The most significant changes involved threat definition, and a separation of probability of attack from probability of success given an attack. Table 3 provides the result of the deliberations.

Table 3. Probability of Success Given an Attack for CDC and Threat

	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
Threat	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
1.	**1.00**	**0.95**	**0.75**	**0.50**	**0.35**	**0.30**	**0.50**	**0.45**	**0.35**	**0.20**	**0.15**	**0.35**	**0.30**	**0.10**	**0.05**
2.	**1.00**	**0.95**	**0.85**	**0.60**	**0.45**	**0.35**	**0.60**	**0.50**	**0.35**	**0.20**	**0.15**	**0.40**	**0.35**	**0.15**	**0.10**
3.	**1.00**	**1.00**	**1.00**	**0.95**	**0.85**	**0.75**	**0.90**	**0.85**	**0.70**	**0.50**	**0.40**	**0.60**	**0.50**	**0.35**	**0.25**

The first column of numbers shows that all of the attackers can easily penetrate the unprotected integrated target environment. As protection mechanisms are added, moving to the right in the table, the probability of success begins to go down. Note that the probabilities of success go up between the integrated defense in depth configuration (DC6) and the baseline separated configuration (DC7). This occurs again between the separated defense in depth configuration (DC11) and the baseline isolated configuration (DC12). The well resourced determined threat (3) has the highest probability of success for any particular defensive configuration. The time limited group (threat 1) have slightly lower probabilities of success than the extortionists (threat 3) because they were judged to have less time to form effective teams and less time for network surveillance and attack planning. Perhaps a more intuitive way to view these probabilities is in terms of the defense posture, or probability of a successful defense against attacks. These probabilities are simply one minus the probability of successful attacks. Figure 13 shows

how the information assurance protection mechanisms added in each stage of defense configurations increase the probability of successful defense. CDC 1 represents a completely undefended system. The drop in defensive posture between CDC 6 and CDC 7 is due to the shift from a well-defended "Integrated" configuration to a minimally defended "Separated" configuration. Similarly, the drop in defensive posture between CDC 11 and CDC 12 is due to the shift from a well-defended "Separated" configuration to a minimally defended "Isolated" configuration.

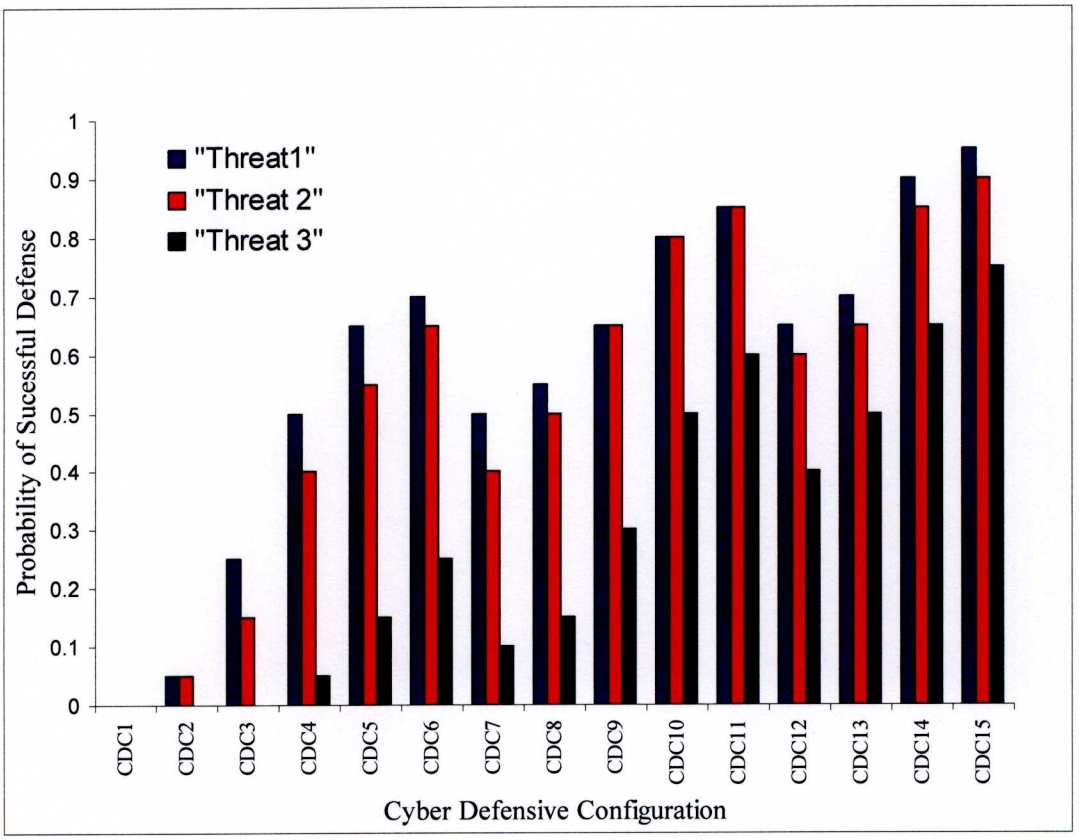

Figure 13. Successful Defense

6.2 Refinements to the Figures

The Delphi Group met over four separate occasions to develop the values for probability of success given an attack (Ps/a). After completion of the task, an analysis was undertaken to refine these figures. Several different approaches were undertaken:

a. Rank Equivalence – The conjecture that a strong defense for one threat should be a strong defense for another threat was proffered. Table 4 shows the relative rankings for the 15 configurations with the strongest defense having the lowest probability of success.

Table 4. Relative Ranking of Defenses

Threat	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
1	1	0.95	0.75	0.5	0.35	0.3	0.5	0.45	0.35	0.2	0.15	0.35	0.3	0.1	0.05
Rank	15th	14th	13th	11th, 12th	7th, 8th, 9th	5th, 6th	11th, 12th	10th	7th, 8th, 9th	4th	3rd	7th, 8th, 9th	5th, 6th	2nd	1st
2	1	0.95	0.85	0.6	0.45	0.35	0.6	0.5	0.35	0.2	0.15	0.4	0.35	0.15	0.1
Rank	15th	14th	13th	11th, 12th	9th	5th, 6th, 7th	11th, 12th	10th	5th, 6th, 7th	4th	2nd, 3rd	8th	5th, 6th, 7th	2nd, 3rd	1st
3	1	1	1	0.95	0.85	0.75	0.9	0.85	0.7	0.5	0.4	0.6	0.5	0.35	0.25
Rank	13th, 14th, 15th	13th, 14th, 15th	13th, 14th, 15th	12th	9th, 10th	8th	11th	9th, 10th	7th	4th, 5th	3rd	6th	4th, 5th	2nd	1st

An inconsistency is noted in red. When presented with this inconsistency and a way to resolve them, is by altering the values slightly. The Delphi team was unanimous in their rejection, noting that the additive effects of configuration and defensive measures may have a multiplying effect and some mechanisms make other mechanisms more useful. For example, IDS in an isolated "quiet" system means any anomaly should be investigated and responded to).

b. Relative Ratios – The conjecture that a defense mechanism applied in one area should provide a relative improvement that would be about the same in other areas was proffered. Table 5 shows the relative difference in Ps/a for additional mechanisms. The table provides the values of improvement for the next element (for example CDC1 to CDC2 improved by 5% for Threats 1 and 2 and not at all for Threat 3). These can be compared across the LAN types. For moving to the managed security posture for Threat 3, the improvement is worth only 5% in the integrated LAN, but worth 21% in the separated LAN and 20% in the isolated LAN. The Table also shows the like to like across LAN types where CDC2 compares to CDC7, CDC3 to CDC8, CDC4 to CDC9, CDC5 to CDC10 and CDC6 to CDC11. Note the switch for separated where Baseline in the isolated is then enhanced and separated, so that CDC8 compares to CDC12, etc. Several values are highlighted as being suspect.

Table 5. Relative Ratios

Threat	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
1	**1.00**	**0.95**	**0.75**	**0.50**	**0.35**	**0.30**	**0.50**	**0.45**	**0.35**	**0.20**	**0.15**	**0.35**	**0.30**	**0.10**	**0.05**
ratio	---	**1.05**	**1.27**	**1.50**	**1.43**	**1.17**	---	**1.11**	**1.29**	**1.75**	**1.33**	---	**1.17**	**3.00**	**2.00**
like-like							**1.90**	**1.67**	**1.43**	**1.75**	**2.00**	**1.29**	**1.17**	**2.00**	**3.00**
2	**1.00**	**0.95**	**0.85**	**0.60**	**0.45**	**0.35**	**0.60**	**0.50**	**0.35**	**0.20**	**0.15**	**0.40**	**0.35**	**0.15**	**0.10**
Rank	---	**1.05**	**1.12**	**1.42**	**1.33**	**1.29**	---	**1.20**	**1.43**	**1.75**	**1.33**	---	**1.14**	**2.33**	**1.50**
like-like							**1.58**	**1.70**	**1.71**	**2.25**	**2.33**	**1.25**	**1.00**	**1.33**	**1.50**
3	**1.00**	**1.00**	**1.00**	**0.95**	**0.85**	**0.75**	**0.90**	**0.85**	**0.70**	**0.50**	**0.40**	**0.60**	**0.50**	**0.35**	**0.25**
Rank	---	**1.00**	**1.00**	**1.05**	**1.12**	**1.13**	---	**1.06**	**1.21**	**1.40**	**1.25**	---	**1.20**	**1.43**	**1.40**
like-like							**1.11**	**1.18**	**1.36**	**1.70**	**1.88**	**1.42**	**1.40**	**1.43**	**1.60**

When presented with these data and a way to resolve them by altering the values slightly, the Delphi team was again unanimous in their rejection, though some deliberation was required. They noted the previous rationale and additionally that having to break multiple levels of defenses is an "AND" effect leading to large changes at times.

c. Cross Plot Smoothing – Given that rankings could be used to order the defense postures from strongest to weakest we could look at a plot of relative strength and look for lumps and/or inconsistencies. Figure 14 provides the basic approach with the ordering being based upon Threat 3. Separate figures need to be developed for each of the orderings since they did not agree, although as shown in the figure, Threats 1 and 2 could be modified to follow Threat 3 ordering. The variations in the plot were not used by the Delphi Group to make changes for reasons already cited.

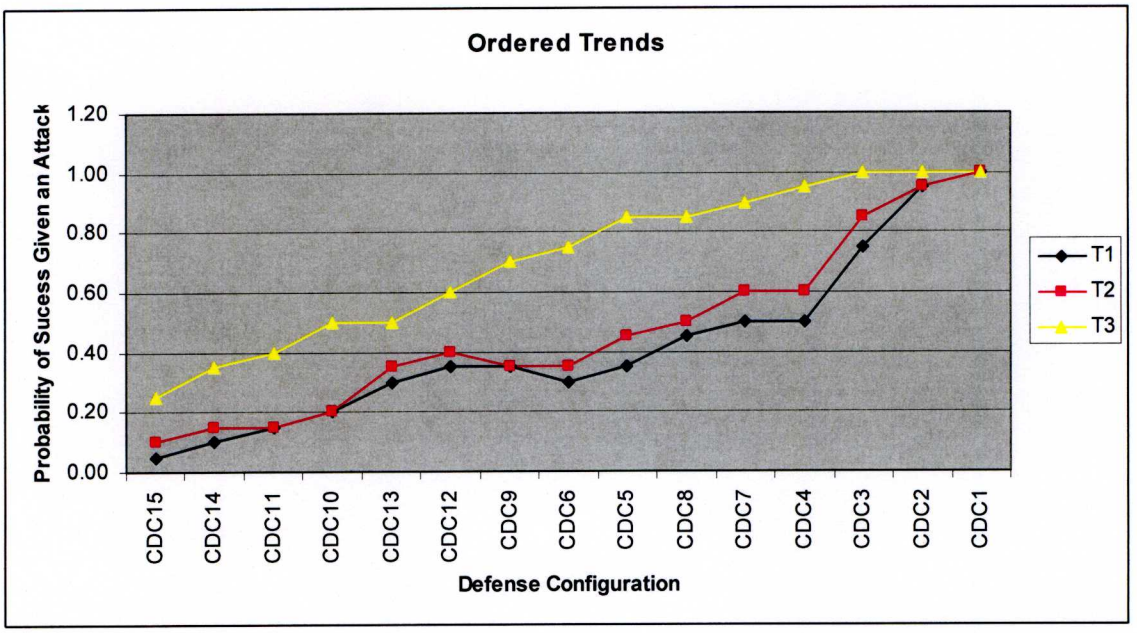

Figure 14. Cross Plot Smoothing

6.3 Probabilities of Success Approximated for Corporate LANS

Section 4.7 developed cyber defensive configurations for the corporate LAN. These mirror Defensive configurations 1-6.

Table 6. Probability of Success Given an Attack for Corporate LAN Configurations

Def. Config.	CDC1	CDC2	CDC3	CDC4	CDC5	CDC6
	Corporate Protection					
Threat	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+
1	**1.00**	**0.95**	**0.75**	**0.50**	**0.35**	**0.30**
2	**1.00**	**0.95**	**0.85**	**0.60**	**0.45**	**0.35**
3.	**1.00**	**1.00**	**1.00**	**0.95**	**0.85**	**0.75**

6.4 Consideration of Best Practices

After developing these configurations it was apparent to the Delphi group that this was insufficient in that violations of best practices could cause the unraveling of the security of the PCS system. It was eventually decided to treat this as a penalty issue to avoid a proliferation of defensive configurations. Five basic violations were examined:

A. RF Connect Without Integrity or Encryption – for purposes of analysis WEP and WAP are not considered encryption.

B. Any Use of USB in PCS Environment – exception may be where USB separately scanned and verified.

C. System Environment Not Physically Protected

D. PCS Not Physically Protected Or Elements not Physically Protected

E. System Internet Connectivity – PCS side.

The penalty alone was insufficient because it may have a varying impact upon the threat. Threats were dealt with in the previous Chapter. The Threats have been placed into three categories. A more capable threat might more easily take advantage of a best practice violation. It was further complicated by the basic configuration of the LAN. After much trial and error a penalty value was developed. Penalties are applied up to a 1.0 Probability of success. This resulted in the Penalty shown in Table 7.

Table 7. Penalty for Violation of Best Practice

Maximum probability of success given attack =1.0	A (RF) (1)Integrated (2) Separated (3) Isolated	B (USB) (1)Integrated (2) Separated (3) Isolated	C (Sys≠Pr) (1)Integrated (2) Separated (3) Isolated	D (PCS≠Pr) (1)Integrated (2) Separated (3) Isolated	E (Internet) (1)Integrated (2) Separated (3) Isolated
1.Criminal Extortionist	100 105 110	100 110 110	120 120 130	110 120 130	100 Not Separated Not Isolated
2.Isolated Terrorist	105 115 125	110 120 130	130 130 130	120 120 130	100 Not Separated Not Isolated
3.Coordinated Terrorist	110 120 130	120 130 140	130 140 150	130 130 150	100 Not Separated Not Isolated

6.5 Computation of Probability of Success Given an Attack

The actual computation of success probability was now based upon three factors:

- Cyber Defensive Configuration
- Threat Being Considered
- Potential Violations of "Best Practice"

7. Matching Survey Responses to the CDCs and Obtaining an Analysis Value of Probability of Success

7.1 Survey Responses

Survey questions were designed to be simple, answered with a yes or no (to reduce ambiguity) and provide a unique match for each of the CDCs. Table D-1 of Appendix D provides the appropriate answers for each of the defined defensive configurations. For a definition of the questions, see Section 4.8, "Survey Questions For Establishing Defensive Configurations for PCS Systems." To demonstrate that each of the CDCs have a unique set of answers to the questions, we can compare the answers in any column to the answers in any other column with the results provided in Table D-2 of Appendix D. The table illustrates that the columns are equal only to themselves. This does not mean, however that the 28 questions cannot be answered in such a way as to not match one of the 13 configurations. This is particularly true for the aspects associated with managed security. A particular asset owner may have implemented only a few or less than all elements under that process. As a result, those answers need to be carefully screened against the CDCs and adjustments made as outlined below.

7.2 Computation

The probability of success given an attack is reduced to a three-factor computation. The first was the defensive configuration as determined by the set of network questions given in Section 4.8, "Survey Questions For Establishing Defensive Configurations for PCS Systems." We first determine configuration type (integrated, separated, isolated) and then the CDC within that grouping. The second factor was the threat being considered, as defined in Section 5 "Threat Scenarios." These two factors will provide a baseline probability of success number. The third factor modifies that number as presented in Section 6.5.

7.3 Example Computations

7.3.1 An Example with a CDC Match

Survey results for a facility, Facility X, have provided the following answers to survey questions:

YES, NO, YES, YES, YES, YES, YES, YES, YES, YES, YES, YES, NO, YES, NO, YES, NO, YES, YES, YES, YES, YES, YES, YES, YES, YES, YES, YES

These survey responses uniquely match CDC10, and the category is separated. The initial probability of success given an attack is drawn directly from Table 3. The values can be gleaned for each of the three threat categories.

- T1 = 0.20
- T2 = 0.20
- T3 = 0.50

If there are no violations of best practice then these numbers can be used directly in the calculation.

7.3.2 An Example without a CDC Match

Survey results for Facility Y have provided the following answers to survey questions:

YES, NO, YES, YES, YES, YES, YES, NO, YES, NO, YES, YES, NO, YES, NO, NO, NO, YES, YES, YES, YES, YES, YES, YES, BLANK, YES, YES, YES

These match no CDC and in fact, notice that one question was unanswered. In order to compute the probability of success given an attack we use a method called nearest neighbor. The nearest neighbor algorithm allows for blank answers as well as inexact matches. In this case the nearest neighbor is CD10 with a mismatch of 4 (that is, 24 of 28 questions match). In the nearest neighbor, we assign a value to the next lowest defense configuration (in the same category). The next lowest (CD9) value obtained from Table 3 is:

- Criminal Extortionist (T1) = 0.35
- Isolated Terrorist (T2) = 0.35
- Coordinated Terrorist (T3) = 0.70

However, this defensive configuration uses RF in the PCS with only WAP protection, which is a violation of the best practices rule, so by applying Table 3, we arrive at the final value of probabilities for each of the threats as:

- Criminal Extortionist (T1) = 0.35*1.05 = 0.37
- Isolated Terrorist (T2) = 0.35*1.15 = 0.40
- Coordinated Terrorist (T3) = 0.70*1.20 = 0.84

8. Consequence Calculation

8.1 Consequence Issues

Consequence data is best calculated by the asset owner, preferably in conjunction with a vulnerability analysis. This is the process that best groups the at-risk assets; accounts for mechanical and personnel backup procedures and provides a realistic representation of the damages that might be caused by a cyber intrusion. Data on cyber attacks is considered sensitive proprietary information within these industries. The consensus from discussions with industry experts at process control professional symposia was that the consequences of cyber attacks on process control systems would be difficult to distinguish from ordinary operational accidents and equipment failures. Routine operational accidents and equipment failures are reported to government monitoring agencies, where data is available. The task here was to present notional consequences that were realistic as a demonstration of the analysis process. In this chapter we list data sources and rationale for the three threat scenarios with a notional electric company and a notional oil and gas company. Consequences of cyber attacks by criminal extortionists and spot terrorists were assumed to be similar in scale and duration to non-weather related operational accidents and equipment failures. Large-scale electrical power outages have been analyzed in the literature, as have major oil and gas supply disruptions caused by hurricanes. Consequences for large-scale cyber attacks by coordinated terrorists were derived from such reports.

8.2 Data Sources

Consequences of cyber attacks were assumed to be similar in scale and duration to non-weather related operational accidents and equipment failures. This was consistent with industry workshop analysis as described in Section 3, "Assessment Modeling Approach." Data for electrical power disruptions was taken from Department of Energy reports for 2005 and 2006[11] and from databases compiled by the North American Electric Reliability Corporation.[12] The average service disruption from this data was a loss of 300 MW of power generation capability for 6 hours, affecting 100,000 customers. These numbers

---

[11] U.S. Department of Energy, Energy Information Administration, "Major disturbances and unusual occurrences," http://www.eia.doe.gov.

[12] North American Electric Reliability Corporation (NERC), Disturbance Analysis Working Group (DAWG), databases for 2000, 2001, and 2002, http://www.nerc.com/~dawg.

form the basis for consequences from both the criminal extortionist and spot terrorist threats.

For the large-scale terrorist threat we used data from two major electrical power outages in 2003, one in the northeastern US and one in Italy. The economic impacts of these disruptions have been thoroughly researched.[13, 14, 15, 16] A simple estimate of overall consequences from lost revenues, cleanup and restoration, lost productivity and wages, and spoilage, according to this research, is 100 times the retail cost of the lost power generation capacity.[17] For these calculations $0.10 per kWh was used as a rough estimate of the retail cost of electrical power.

Data for gas pipeline disruptions was taken from Department of Transportation reports for 2002 to 2007.[18] The average service disruption from natural gas pipeline ruptures according to this data was a 2-hour outage with $800K in property damage and $200K worth of lost gas. Incidents where fires or explosions are sparked roughly double these losses.

There is relatively little economic impact from small gas pipeline disruptions. Unlike electrical power distribution systems, which have no storage capacity, gas distribution systems include storage facilities along their route from which gas can continue to be pumped when the supply is halted. Gas prices may increase during extended pipeline outages if the demand exceeds stored supplies. Even when significant supply lines are stopped for extended periods, though, the retail cost of gas increases by less than a factor of 2.[19]

---

[13] Anderson Economic Group, "Northeast blackout likely to reduce U.S. earnings by $6.4 billion," August 2003, http://andersoneconomicgroup.com.

[14] Electricity Consumers Resource Council, "The economic impacts of the August 2003 blackout," ELCON, February 2004, http://www.elcon.org.

[15] ICF International, "The economic cost of the blackout," ICF Consulting, August 2003, http://www.icfi.com.

[16] Lawrence Berkeley National Laboratory, Kristina LaCommare and Joseph Eto, "Cost of power interruptions to electricity consumers in the United States," LBNL-58164, February 2006," http://www.lbl.gov.

[17] ICF International, *op cit.*

[18] U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration, Office of Pipeline Safety statistics database, http://ops.dot.gov.

[19] U.S. Department of Energy, Energy Information Administration, "A look at western natural gas infrastructure during the recent El Paso pipeline disruption," November 2000, http://www.eia.doe.gov.

8.3 Threat 1 – Electrical Power Disruption

Cyber attacks against electrical power systems by the small terrorist cell were launched without warning. The attacks manipulated generation thresholds, creating power surges and triggering physical protection mechanisms that cutoff segments of the power distribution grid. This incident was timed during mid-winter, which led to three deaths from lost heating capacity, stranded travelers, and increased risk to emergency responders.

These disruptions were assumed to cut off 300 MW of power generation capability. Half of this capacity would be restored in 2 hours. Using straight-line recovery approximations (see Figure 15) this leads to 450 MWh of power lost during the first 2 hours and 300 MWh lost during the second 4 hours, for a total loss of 750 MWh. The lost revenue from 750 MWh of power would be $75K, with an extended economic impact of $7.5M. The three deaths add $22.5M to produce a total economic impact for this incident of $30.0M.

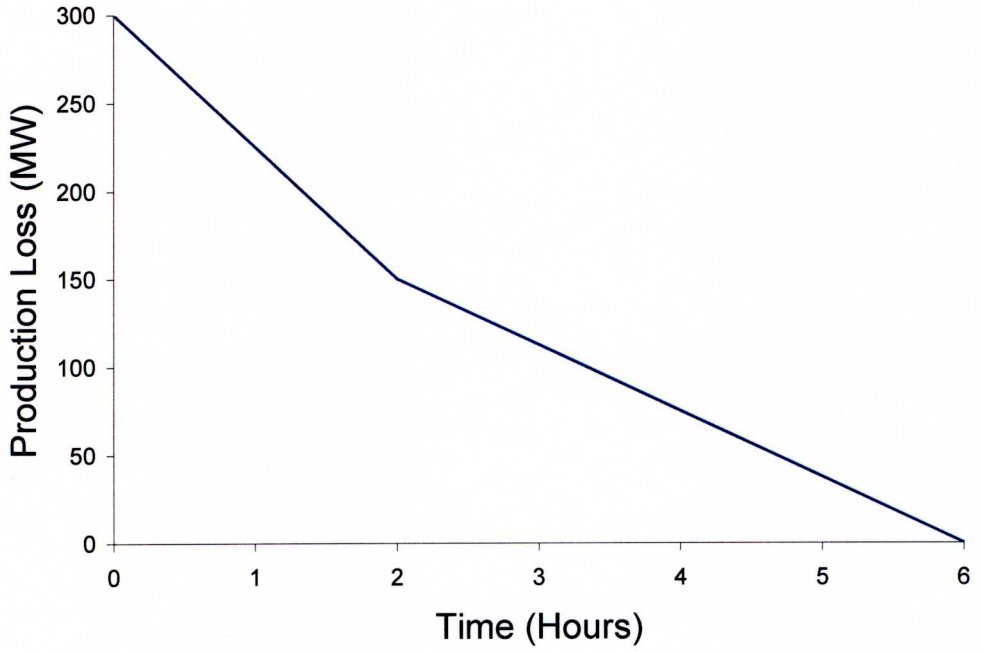

Figure 15. Notional Production Loss from Spot Terrorist Attack

8.4 Threat 1 – Gas Pipeline Disruption

Cyber attacks against natural gas distribution systems by the small terrorist cell were launched without warning. The attacks manipulated pressure regulation thresholds, causing pressure fluctuations and rupturing a segment of 16-inch pipeline. Fire sparked by the incident contributed significantly to the damage. One death in fighting the fire was attributed to this incident.

These disruptions were assumed to cause $1.9M of property damage, in addition to $400K worth of gas that escaped from the ruptured pipe before isolation valves were closed. The increased costs over the criminal extortionist example are due to the fire. Direct losses for the pipeline operator, therefore, come to $2.3M. The one death adds $7.5M for a total impact of $9.8M.

8.5 Threat 2 – Electrical Power Disruption

Cyber attacks launched against electrical power systems by the criminal extortionists were assumed to manipulate generation thresholds, creating power surges and triggering physical protection mechanisms that cutoff segments of the power distribution grid. Reconnecting the isolated grid segments requires work crews to climb power poles and replace fuse links. Power surges may also damage transformers on pole tops and at distribution hubs. Replacement equipment requires time to locate and transport to the work sites. No injuries or loss of life were attributed to this power outage.

These disruptions were assumed to cut off 300 MW of power generation capability. Half of this capacity would be restored in 2 hours. Using straight-line recovery approximations this leads to 450 MWh of power lost during the first 2 hours and 300 MWh lost during the second 4 hours, for a total loss of 750 MWh. The lost revenue from 750 MWh of power would be $75K at $0.10 per KWh. The total economic impact for this incident, therefore, is on the order of $7.5M.

8.6 Threat 2 – Gas Pipeline Disruption

Cyber attacks launched against natural gas distribution systems by the criminal extortionists were assumed to manipulate pressure regulation thresholds, causing pressure fluctuations and rupturing a segment of 16-inch pipeline. No fire or explosion was created. Restoring the pipeline requires work crews to repair or replace damaged segments of pipe, which may be underground or otherwise difficult to access. Replacement equipment requires time to locate and transport to the work site. No injuries or loss of life were attributed to this incident.

These disruptions were assumed to cause $800K of property damage in addition to $200K worth of gas that escaped from the ruptured pipe before isolation valves were closed. Direct losses for the pipeline operator, therefore, come to $1.0M. Because of gas storage facilities that can continue to supply gas there was little if any disruption of gas flow to most customers.

8.7 Threat 3 – Electrical Power Disruption

Cyber attacks against multiple electrical power systems by the large terrorist group were launched without warning. The attacks manipulated generation thresholds, creating power surges and triggering a cascade of equipment failures and damage to multiple high-voltage transformers. This incident was timed during mid-winter, which led to

twenty deaths from lost heating capacity, stranded travelers, and increased risk to emergency responders.

These disruptions were assumed to cut off 60,000 MW of power generation capability. Half of this capacity would be restored in 4 hours. The remaining power would be restored in stages as shown in Table 8 and Figure 16. Notional Production Losses for Large-Scale Terrorist Attack over a total of 72 hours. Using straight-line recovery approximations this leads to a total loss of 697,500 MWh. The lost revenue from this outage would be $69.75M, with an extended economic impact of $6,975M. The twenty deaths add $150M to come up with total economic impact for this incident of $7,125M.

Table 8. Recovery schedule for a major electrical power outage

Initial outage 60,000 MW	Generation Lost	Revenue Loss
50% recovered after 4 hours	180,000 MWh	$18M
75% recovered after 12 hours	180,000 MWh	$18M
88% recovered after 24 hours	135,000 MWh	$13.5M
97% recovered after 48 hours	135,000 MWh	$13.5M
99% recovered after 72 hours	67,500 MWh	$6.75M
Total power and revenue loss	697,500 MWh	$69.75M

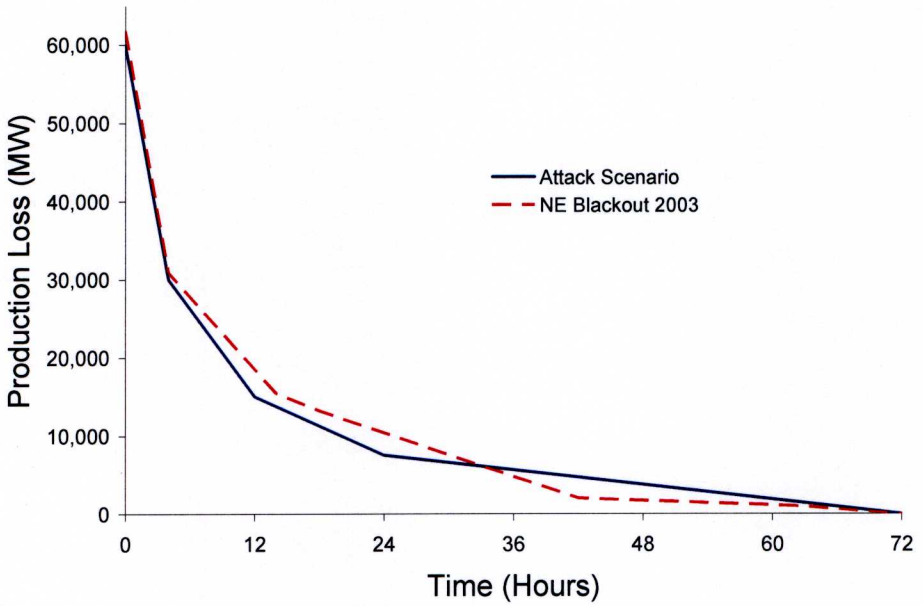

Figure 16. Notional Production Losses for Large-Scale Terrorist Attack

8.8 Threat 3 – Oil Platform Disruption

Cyber attacks against an offshore oil-drilling platform by the large terrorist group were launched without warning. The attacks manipulated the ballast system on a semi-submersible oil platform to flood ballast tanks on one side and emptying them on the other side. This caused the platform to capsize and sink during a tropical storm. Twenty-

five of the 80 people on board the platform died in the incident. The platform is a total loss and has a 12-month replacement time.

Cost estimates for this incident were based on oil platform damage data from Hurricane Katrina.[20] Ballast systems were not affected by Katrina, but several semi-submersible platforms broke loose from their moorings and were damaged or destroyed. Ballast systems are controlled by automated control systems like those described in this report. We assumed there were network connections to these systems, at least for reporting system health and status off-platform, back to corporate operations monitors. This provided the path for the cyber attackers to penetrate the control system.

Replacement cost of the oil platform was estimated to be on the order of $350M. The 12 months of oil production loss was estimated to cost the operator an additional $54.75M. The 25 deaths add another $187.5M for a total impact of $595.25M.

[20] Rigzone, "Special Report: Hurricane Katrina Damage Assessment," September 2005, http://www.rigzone.com.

9. Conditional Risk Calculations

The conditional risk is the product of the probability of success, given an attack, and the consequences that would result from an attack. The following tables combine the probabilities of success for each threat from Section 6 and the economic consequences for each cyber attack scenario from Section 8, using the conditional risk formulation presented in Section 3.

9.1 Spot Terrorist Threat 1

Table 9 shows the probability of success and conditional risk for the spot terrorist threat of electrical power disruption and gas pipeline disruption by cyber attack. Figure 17 plots these two sets of conditional risks for comparison. As before, the Conditional Risk generally drops within the three basic configurations as cyber defenses are strengthened, but at the boundary the trend may reverse indicating that the weaker configurations of the separated and isolated may be less desirable than a stronger configuration of the previous category. However, the larger values emphasize the need to seek higher levels of cyber defense.

Table 9. Conditional Risk for the Spot Terrorist

Defense Config.	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
Probability of Success	1.00	0.95	0.75	0.50	0.35	0.30	0.50	0.45	0.35	0.20	0.15	0.35	0.30	0.10	0.05
Conditional Risk of Electrical Power Disruption - $M	$30.0	$28.5	$22.5	$15.0	$10.5	$9.0	$15.0	$13.5	$10.5	$6.0	$4.5	$10.5	$9.0	$3.0	$1.5
Conditional Risk of Gas Pipeline Disruption - $M	$9.80	$9.31	$7.35	$4.90	$3.43	$2.94	$4.90	$4.41	$3.43	$1.96	$1.47	$3.43	$2.94	$0.98	$0.49

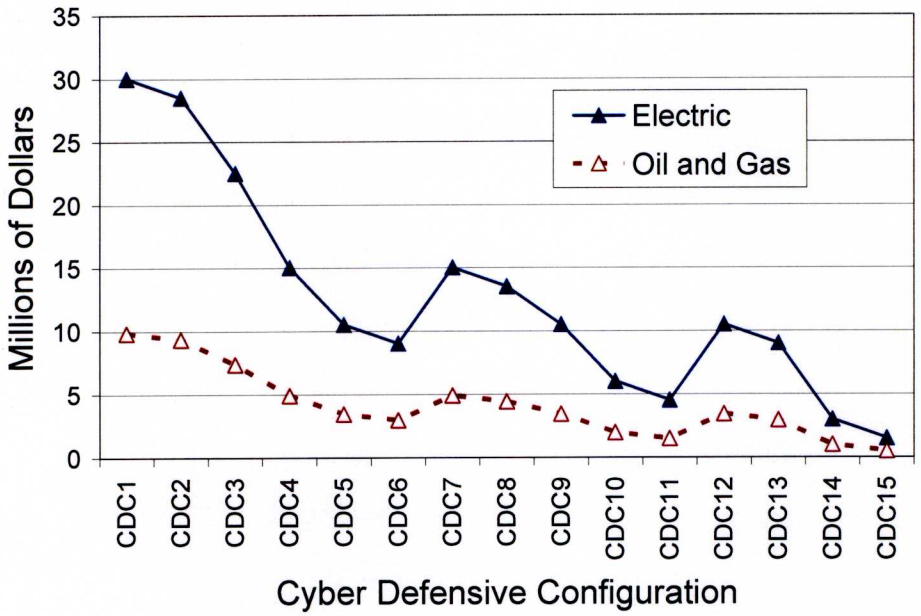

Figure 17. Conditional Risk for the Spot Terrorist Threat

9.2 Criminal Extortion Threat 2

Table 10 shows the probability of success and conditional risk for the criminal extortion threat of electrical power disruption by cyber attack. Figure 18 plots the two sets of conditional risks for comparison. The Conditional Risk generally drops within the three basic configurations as cyber defenses are strengthened, but at the boundary the trend may reverse indicating that the weaker configurations of the separated and isolated may be less desirable than a stronger configuration of the previous category.

Table 10. Conditional Risk for the Criminal Extortion

Defense Config.	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
Probability of Success	1.00	0.95	0.85	0.60	0.45	0.35	0.60	0.50	0.35	0.20	0..15	0.40	0.35	0.15	0.10
Conditional Risk of Electrical Power Disruption - $M	$7.50	$7.12	$6.38	$4.5	$3.38	$2.63	$4.50	$3.75	$2.62	$1.50	$1.13	$3.00	$2.62	$1.12	$0.75
Conditional Risk of Gas Pipeline Disruption - $M	$1.00	$0.95	$0.85	$0.60	$0.45	$0.35	$0.60	$0.50	$0.35	$0.20	$0.15	$0.40	$0.35	$0.15	$0.10

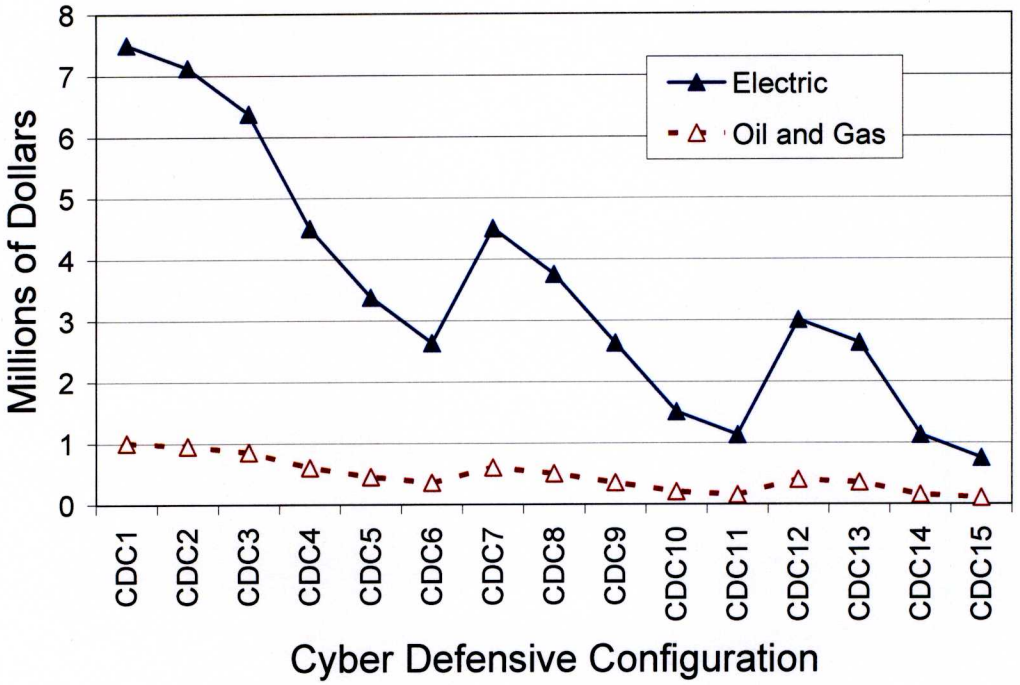

Figure 18. Conditional Risk for Cyber Extortion

9.3 Coordinated Terrorist Threat 3

Table 11 shows the probability of success and conditional risk for the coordinated, large-scale terrorist threat of electrical power disruption and oil platform disruption by cyber attack. Figure 19 plots these two sets of conditional risks for comparison. As before, the Conditional Risk generally drops within the three basic configurations as cyber defenses are strengthened, but at the boundary the trend may reverse indicating that the weaker configurations of the separated and isolated may be less desirable than a stronger configuration of the previous category. However, the larger values emphasize the need to seek higher levels of cyber defense. Note that in all three scenarios improving the overall defense posture reduces conditional risk and at this level of threat even a small amount of improvement makes a large reduction in marginal risk. The ultimate goal of CDC13 or beyond still provides a fair degree of conditional risk for this threat even though the consequence of the oil platform was nearly $600M, the consequence of electrical power disruption was much greater.

Table 11. Conditional Risk for the Large-Scale Terrorist Threat

Defense Config.	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
	Integrated						Separated					Isolated			
	None	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Enhanced	Managed	Def. in Depth	Def. in Depth+	Baseline	Managed	Def. in Depth	Def. in Depth+
Probability of Success	1.00	1.00	1.00	0.95	0.85	0.75	0.90	0.85	0.70	0.50	0.40	0.60	0.50	0.35	0.25
Conditional Risk – Electric Power Disruption - $B	$7.12	$7.12	$7.12	$6.77	$6.06	$5.34	$6.41	$6.06	$4.99	$3.56	$2.85	$4.28	$3.56	$2.49	$1.78
Conditional Risk – Oil Platform Disruption - $m	$595	$595	$595	$565	$506	$446	$536	$506	$416	$298	$238	$357	$298	$208	$149

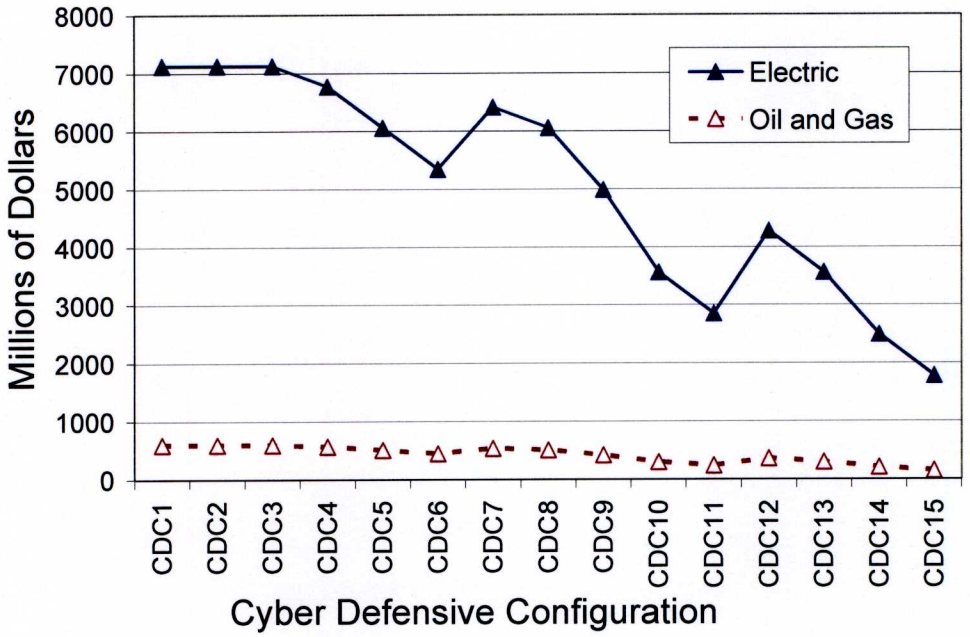

Figure 19. Conditional Risks for the Large-Scale Terrorist Threat

10. Conclusions

10.1 The Following Conclusions Are Derived From This Analysis

- Objectively identifying Cyber Defensive Configurations is possible through the use of simple questionnaires. [Answering the questions may not be so simple.]
- The definition of an asset must be developed by elements of the infrastructure and the asset owner.
- Actual accident/incident data provide an excellent start for consequence data.
- Consequence data are best developed by asset owners.
- The Common Risk Model can be applied to cyber intrusion scenarios.
- The Common Risk Model should only be used for relative ranking of cyber conditional risks and the absolute values computed may contain inaccuracies.
- Probabilities of success given an attack, while subjective, represent reasonable relative positions of cyber defense effectiveness.

11. Recommendations

11.1 The Following Recommendations Are Made:

- Threat attributes and potential threats for these analyses should be separated and deliberately crafted.
- The analysis should be extended to the general case of IT infrastructure as part of a critical infrastructure operation. This analysis was limited to the process control system aspects.
- The analysis process should be made available to asset owners in the critical infrastructure with training as needed.
- This analysis process for cyber security should be refined by successive iteration and input from asset owners.
- Specific asset owners should be selected to create working examples for the purpose of developing Return on Investment (ROI) models for security measures.

Appendix A.
Definitions and Acronyms

Air Gap Communication by physically moving data between locations.

Access Control In the context of cyber security, access control means limiting access to resources (hardware and software) and information. One of the most common access control mechanism is provided by password logins and/or biometric identification.

Assurance Grounds for confidence that an entity meets its security objectives.

Attack Potential Perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources, and motivation.

Availability Availability is timely, reliable access to data and information services for authorized users. A popular attack is called Denial of Service (DOS), which attempts to make access unavailable

ASD Assistant Secretary of Defense

Best Practices Processes, practices, and systems identified in public and private organizations that performed exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas. Successfully identifying and applying best practices can reduce business expenses and improve organizational efficiency.

Black List A list of unacceptable communications for a computer or network

CC Common Criteria – an ISO Standard for computer security product evaluation

CDC Cyber Defense Configuration

CDC_C Cyber Defense Configuration for Corporate LAN

CIP Critical Infrastructure Protection

CNA Computer Network Attack

CND Computer Network Defense

COCOM Combatant Command (Command Authority)

Computer Security (1) Preventing, detecting, and minimizing the consequences of unauthorized actions by users (authorized and unauthorized) of a computer system. (2) Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Confidentiality The confidentiality security service is defined as preventing unauthorized disclosure of data (both stored and communicated). Confidentiality services will prevent disclosure of data in storage, or transiting. One of the most common confidentiality mechanisms is the use of cryptography.

Consequence Cost of successful cyber attack
CRM Common Risk Model
CRS

Cybersecurity The prevention of damage to, the protection of, and the restoration of computers, electronic communications systems, electronic communication services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

Cyberterrorism A criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies

DARPA Defense Advanced Research Projects Agency

Data Integrity Property that data has not been altered or destroyed in an unauthorized manner

Delphi Process of arriving at agreement among a group of experts. In this study we did a modified Delphi where the agreement was by consensus.

DHS Department of Homeland Security
DIAP Defense- wide Information Assurance Program
DMZ De-militarized zone. In cyber speak this is a buffer area to protect assets.
DoD Department of Defense
DoDI Department of Defense Instruction
DOS Denial of Service
DOT Department of Transportation
DSB Defense Science Board
ET&A Education, Training, and Awareness
Firewall A computer program that limits access and information flow
Honeypot A simplified intrusion detection device
I3P Institute for Information Infrastructure Protection
IA Information Assurance
ICS Industrial Control System
IDA Institute for Defense Analyses
IDS Intrusion Detection System

Insider Entity (e.g., a person) in a computer system who has been given access and trust, but may violate that trust

Integrated Two parts are logically and physically attached

Integrity The integrity security service includes; prevention of unauthorized modification of data (both stored and communicated), detection and notification of unauthorized modification of data, and recording of all changes to data. One of the most common mechanisms for integrity is check sums, or hash algorithms. In some cases independent certification authorities are used

Intrusion Detection Computer program or computer hardware or both that monitors traffic flow for unauthorized activity.

Information Assurance Conducting those operations that protect and defend information and information systems by ensuring availability, integrity, authentication,

confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities

Information Technology Security All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, authenticity, and reliability

Integrity Prevention of unauthorized modification of information

ISO International Standards Organization

Isolated Two parts are neither physically nor logically attached.

IT Information Technology

Knock-on Secondary and tertiary effects that are not a part of the asset consequence calculation.

LAN Local Area Network

MODBUS Modular serial interface

Near Real-Time Monitoring and control happen after the system is progressing by some time.

Nonrepudiation The nonrepudiation security service provides the ability to prove to a third party that the entity did indeed participate in the communication. Some firewalls may refuse communication with parties for which it cannot verify the origin

NERC North American Electric Reliability Council

Network Security Protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats

NIAP National Information Assurance Program

NIPP National Infrastructure Protection Plan

NRC Nuclear Regulatory Commission

NYU New York University

Operations Security The implementation of standardized operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to (1) maintain a system in a known secure state at all times, and (2) prevent accidental or intentional theft, destruction, alteration, or sabotage of system resources

P Probability

P(a) Probability of attack

P(s/a) Probability of success given an attack

PCS Process Control System

PCSF Process Control Systems Forum

PDD Presidential Decision Direction

PLC Program Logic Controller

Rc Conditional Risk is the Risk conditioned upon an attack taking place.

Real-Time Monitoring and control happen as the system is progressing.

Residual Risk (1) Portion of risks remaining after security measures has been applied. (2) Risk that remains after safeguards have been implemented.

RF Radio Frequency or wireless communication

Risk (1) Combination of the likelihood that a threat will be carried out and the severity of the consequences should it happen. (2) Potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets

Risk Assessment (1) Process of analyzing threats to and vulnerabilities of an IT system and the potential impact the loss of information or capabilities of a system would have; the resulting analysis is used as the basis for identifying appropriate and cost-effective countermeasures. (2) Process of identifying security risks, determining their magnitude, and identifying areas requiring safeguards

Risk Management (1) Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected. (2) The entire process of identifying, controlling, and eliminating or minimizing uncertain events that may affect IT system resources

ROI Return On Investment

SCADA Supervisory Control and Data Acquisition

Separated Two parts are logically attached but not physically attached

TCSEC Trusted Computer Security Evaluation Criteria

Threat (1) Any circumstance or event with the potential to harm an IT system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service. (2) Potential danger that a vulnerability may be exploited intentionally, triggered accidentally, or otherwise exercised. (3) A potential cause of an unwanted incident which may result in harm to a system or organization

USB Universal Serial Bus

Vulnerability Weakness in the design, operation, or operational environment of an IT system or product that can be exploited to violate the intended behavior of the system relative to safety, security, and/or integrity

VPN Virtual Private Network

WAN Wide Area Network

WAP Low level encryption protocol for wireless connectivity

WEP Low level encryption protocol for wireless connectivity

White List A list of acceptable communications for a computer or network

Appendix B.
References

U.S. Department of Homeland Security, *National Infrastructure Protection Plan*, Washington DC, 2006.

J. D. Morgeson, et al., Institute for Defense Analyses, National Comparative Risk Assessment Pilot Project, IDA Document D-3309, 2006.

Rae Zimmerman, et al., *Understanding Trends, Causes and Consequences of Failures and Attacks on Oil & Gas Pipeline Infrastructure Systems*, New York University, I3P Process Control Systems Security Workshop, February 15, 2007, Houston, Texas

IDA Paper P-4009, *"Evaluation and Review of the National Information Assurance Partnership (NIAP),"* Institute for Defense Analyses, Gregory N. Larsen et al.,

Lawrence Berkeley National Laboratory, Kristina LaCommare and Joseph Eto, "Cost of power interruptions to electricity consumers in the United States," LBNL-58164, February 2006. http://www.lbl.gov

Library of Congress, Congressional Research Service, "The economic impact of cyber attacks," CRS report for Congress, April 2004. http://www.opencrs.com

North American Electric Reliability Corporation (NERC), Disturbance Analysis Working Group (DAWG), DAWG databases for 2000, 2001, and 2002, http://www.nerc.com/~dawg

Rigzone, Special Report: Hurricane Katrina Damage Assessment, September 2005. http://www.rigzone.com

U.S. Congress, Office of Technology Assessment, "Physical vulnerability of electric systems to natural disasters and sabotage," OTA-E-453, June 1990. http://www.wws.princeton.edu/ota

U.S. Department of Energy, Energy Information Administration, "Major disturbances and unusual occurrences," http://www.eia.doe.gov

U.S. Department of Transportation, Pipeline and Hazardous Materials Safety Administration, Office of Pipeline Safety statistics database, http://ops.dot.gov

Joe Weiss, Applied Control Solutions, LLC, Personal communication, major disaster scenario, joe.weiss@realtimeacs.com

Zimmerman, R., J. Simonoff, and C. Restrepo, NYU, "Understanding Trends, Causes and Consequences of Failures and Attacks on Oil & Gas Pipeline Infrastructure Systems," presented at I3P Process Control Systems Security Workshop, Houston, Texas, February 2007. rae.zimmerman@nyu.edu

Appendix C.
Delphi Participants and Relevant Experience

Dr. Reginald N. Meeson

- Participated in IA assessments conducted by DOT&E during COCOM exercises
  - Overarching assessment of Red Team and Blue Team processes across Service Operational Testing Agencies and Information Warfare Centers
  - Developed effectiveness metrics for IA Red Team activities
- Developing job descriptions and certification requirements for IA assessment
- Red Teams and Blue Teams for addition to DODI 8570 Developed IA metrics framework for Joint Staff Contributed to IA metrics development for ASD NII/DoD-CIO
- Participated as assessment referee in DARPA IA Red Teaming exercise

Dr. Edward A. Schneider

- Adjunct at George Mason University and U of Maryland teaching graduate courses in Network Security and Software Assurance
- Lead for several studies in security architectures
- Validator for NIAP Common Criteria Program
- Member of certification team for Missile Defense Agency network
- Helped define requirements for Information Assurance coordination system
- Conducted study of training for Red Team members across DoD
- Committee member for Annual Computer Security Application Conference

Dr. William R Simpson

- Government member of product evaluation team under Orange Book (TCSEC)
- Reviewer and implementer of the ISO Standard for Security Product Evaluation (Common Criteria)
- Team member for initial launch of National Information Assurance Partnership (NIAP)
- Study team lead on US and DoD efforts in Information Assurance
- Validator for six years under the NIAP Common Criteria Program

- Analysis team member on computer intrusion damage assessment analysis
- Analysis team member on task force for cyber forensics
- Analysis team member on study for intrusion analysis, target assessment and threat assessment on a series of breaches of defense computers

Mr. David A.Wheeler

- Lead evaluator for multiple Common Criteria (CC) evaluations under National Information Assurance Partnership (NIAP)
- Created and graded tests for NIAP CC lab certification
- Author of book on developing secure software
- Developer of software to scan software source code for security vulnerabilities
- Author of research paper describing new technique for countering "Trusting Trust" attack
- Lead on IDA trusted path research
- Analysis team member for work on software and system assurance

Dr. Gregory N. Larsen

- Experienced in analysis of information and cyber warfare, including National Military Strategy to Operate in Cyberspace
- Numerous projects in information assurance
- Developed analysis of cyber aspects of physical security
- Participant in the Defense-wide Information Assurance Program (DIAP)
- Involved in numerous studies involving Defense Science Board (DSB) on related subjects
- Adjunct at University of Tennessee/Laboratory for IT (forensics)
- Previously special consultant to Tennessee Valley Authority
- Previously Director of International Center for Applications of IT, and Director of Telecommunications Applications Partnership at the University of Tennessee

Appendix D.
Questionnaire Data Relevance

Table D-1. Survey Questions Answered for Each of the CDCs

?	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
1	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	NO	NO	NO	NO
2	YES	YES	YES	YES	YES	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO
3	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
4	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
5	NO	NO	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
6	NO	NO	YES	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
7	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	YES
8	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	YES
9	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	YES
10	NO	NO	NO	YES	YES	YES	NO	NO	YES	YES	YES	NO	YES	YES	YES
11	NO	NO	NO	NO	YES	YES	NO	NO	NO	YES	YES	NO	NO	YES	YES
12	NO	NO	NO	NO	YES	YES	NO	NO	NO	YES	YES	NO	NO	YES	YES
13	NO	NO	NO	NO	NO	NO	YES	YES	YES	YES	YES	NO	NO	NO	NO
14	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	YES	YES	YES	YES
15	NO	NO	NO	NO	NO	YES	NO	NO	NO	NO	YES	NO	NO	NO	YES
16	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
17	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
18	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
19	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES	YES
20	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
21	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
22	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
23	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
24	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
25	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
26	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
27	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES
28	NO	NO	NO	YES	YES	YES	NO	YES	YES	YES	YES	YES	YES	YES	YES

Table D-2. CDC Uniqueness Test

	CDC 1	CDC 2	CDC 3	CDC 4	CDC 5	CDC 6	CDC 7	CDC 8	CDC 9	CDC 10	CDC 11	CDC 12	CDC 13	CDC 14	CDC 15
CDC1	True	False	False	False	False	False	False	False	False	False	False	False	False	False	False
CDC2	False	True	False	False	False	False	False	False	False	False	False	False	False	False	False
CDC3	False	False	True	False	False	False	False	False	False	False	False	False	False	False	False
CDC4	False	False	False	True	False	False	False	False	False	False	False	False	False	False	False
CDC5	False	False	False	False	True	False	False	False	False	False	False	False	False	False	False
CDC6	False	False	False	False	False	True	False	False	False	False	False	False	False	False	False
CDC7	False	False	False	False	False	False	True	False	False	False	False	False	False	False	False
CDC8	False	False	False	False	False	False	False	True	False	False	False	False	False	False	False
CDC9	False	False	False	False	False	False	False	False	True	False	False	False	False	False	False
CDC10	False	False	False	False	False	False	False	False	False	True	False	False	False	False	False
CDC11	False	False	False	False	False	False	False	False	False	False	True	False	False	False	False
CDC12	False	False	False	False	False	False	False	False	False	False	False	True	False	False	False
CDC13	False	False	False	False	False	False	False	False	False	False	False	False	True	False	False
CDC14	False	False	False	False	False	False	False	False	False	False	False	False	False	True	False
CDC15	False	False	False	False	False	False	False	False	False	False	False	False	False	False	True

Appendix E.
Validation Review Data

Working Definitions

Validation. The purpose of the workshop is to independently review the Probability of Success given an Attack. Estimates developed by IDA and confirm their 1) logical consistency and 2) coherence.

Logical Consistency. Logical consistency is established for both the rank order of overall defensive configurations (ODCs) and the rank order for the estimates probability of success given an attack (P(s/a) for the ODCs based on the description of a given attack type. The rank order within a given defensive layer is sequenced from strongest (most likely to defeat the attack) to weakest (least likely to defeat the attack). The rank order of ODCs based on their attributes is consistent if the following conditions are met: 1) the ODC with all the attributes ranks on the strongest end of the ordering; the ODC with none of the attributes available for that layer ranks on the weakest end of the ordering; 2) any ODC with a proper subset of attributes of another ODC ranks weaker. In all other cases rank order cannot be established. The rank order of P(s/a)s based on probability estimates must be consistent with the rank order of the ODCs based on attributes. All P(s/a)s with the same set of attributes must have the same P(s/a) estimate. *Note that this allows for ODCs that are indistinguishable with respect to rank order based on attributes to have a distinguishable rank order based on the probability estimates. Analyzing cyber attacks, cyber defense configurations (CDCs) have been defined in a manner that is consistent with the definitions of ODCs for defense against physical attacks.*

Coherence. Coherence is established when any pair wise comparison of P(s/a)s for two ODCs and a given attack type are deemed reasonable and based on acceptable supporting evidence. *Note that validation depends on the consensus of the validation group that the ratio comparison of a given pair wise comparison of two P(s/a) estimates is unreasonable or not supportable by the evidence provided.*

Summaries of Validation Meeting Participants

Chris Barrett, Ph.D.

Director, Network Dynamics & Simulation Science Laboratory Virginia Bioinformatics Institute

Professor, Virginia Bioinformatics Institute and Department of Computer Science, Virginia Tech

Ph.D, Bioinformation Systems, Caltech 1985

Served as a submarine officer from 1976 to 1981
Founded the Decision Aids Research Team at the Naval Air Development Center
Study areas: self-organizing sensor systems, communication systems and intelligent control systems, high performance computing based, agent-oriented simulation of very large systems
Founded the Basic and Applied Simulation Science Group in the Computational and Computer Science Division at Los Alamos National Lab

Newton Howard, Ph.D.

Research Professor, The George Washington University and at the Rochester Institute of Technology
Doctoral degree in Cognitive Informatics from La Sorbonne, France
Faculty of Mathematical Sciences at the University of Oxford
Research Professor in Mathematics, Informatics, and Psychiatry
Senior Research Professor at the Cyber Security Policy Research Institute
Holds multiple U.S. patents, and is the author of several publications in the areas of military information science, computer systems theory, and strategic thinking

Michael B. Lombard

Senior Associate, Technology & Management Services, Inc.
Cyber security consultant, National Cyber Security Division of the Department of Homeland Security
Former: Director of Critical Infrastructure Protection/Cyber Security Strategic Initiatives in the National Cyber Security Division of the Department of Homeland Security
Former: Chief of the Control Systems Section in the Protective Security Division of DHS
Former: Deputy Director for Infrastructure Security Analysis, with the Critical Infrastructure Assurance Office of the White House
Former: Information Technology Security Manager for the Department of Commerce, and as Commerce

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
June 2007	Study	

4.	5a. CONTRACT NUMBER
National Comparative Risk Assessment Pilot Project Cyber Intrusion Analysis– Process Control Systems	DASW01-04-C-0003
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS
6. AUTHOR(S)	5d. PROJECT NUMBER
William R. Simpson, Reginald N. Meeson	
	5e. TASK NUMBER
	ER-6-2474
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBERI
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	IDA Paper P-4226
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Risk Management Division Department of Homeland Security 1110 North Glebe Road Arlington, VA 22201	DHS
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; unlimited distribution: 17 October 2007.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The Homeland Security Act of 2003 and the Homeland Security Presidential Directive 7 call for the Department of Homeland Security to conduct comprehensive assessments of the nation's critical infrastructure as well as establish uniform policies, approaches, guidelines and methodology for integrating Federal infrastructure and protection and *risk management* activities. An initial pilot project was undertaken to define a common risk model with common methodologies and approved scales to measure key parameters to accelerate the progress toward the stated goals of the Department in risk assessment activities. This report describes an extension of that analysis to the area of Risk Assessment for Cyber attacks. This involves defining cyber threats, the basic building blocks of security systems, and Cyber Defensive Configurations (CDCs) that are made up of the building blocks and are reasonable representations of actual systems, the development of scenarios for consequence evaluation, and providing notional examples of the computations.

15. SUBJECT TERMS

Cyber Defense, Risk Assessment, Critical Infrastructure, Common Risk Model, Cyber Terrorism, Process Control Systems, SCADA, PCS, ICS, Probability, Consequence Data

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Mr. Matthew Bettridge
Unclassified	Unclassified	Unclassified	Unlimited	82	19b. TELEPHONE NUMBER (Include Area Code) 703-235-5495